

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2001-352321

(43)Date of publication of application : 21.12.2001

(51)Int.Cl.

H04L 9/08

G06F 12/14

(21)Application number : 2000-179695

(71)Applicant : SONY CORP

(22)Date of filing : 15.06.2000

(72)Inventor : ISHIGURO RYUJI

OSAWA YOSHITOMO

OISHI TAKEO

ASANO TOMOYUKI

MITSUZAWA ATSUSHI

(30)Priority

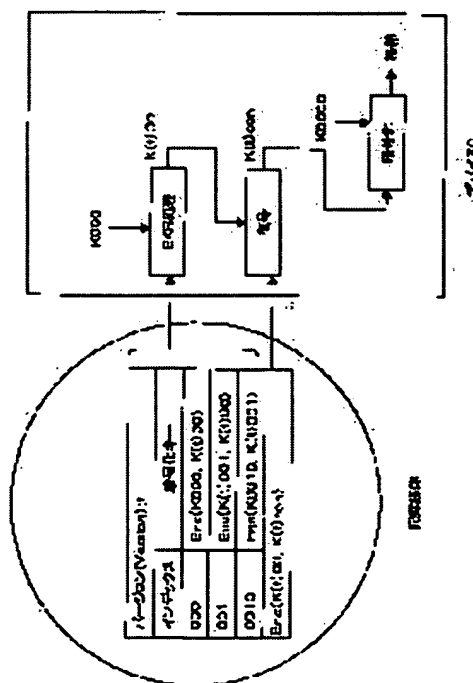
Priority number : 2000105329 Priority date : 06.04.2000 Priority country : JP

(54) INFORMATION PROCESSING SYSTEM, INFORMATION PROCESSING METHOD, AND INFORMATION RECORDING MEDIUM, AND PROGRAM PROVIDING MEDIUM

(57)Abstract:

PROBLEM TO BE SOLVED: To realize an information processing system and its method that execute distribution of various keys or data through an encryption key configuration adopting a tree structure so as to attain efficient and secure data distribution.

SOLUTION: A contents key, an authentication key, and program data or the like adopting an encryption key configuration employing a tree structure are transmitted with an effective key block(EKB). The EKB is configured to allow a device being a leaf of a tree to store a leaf key and a limited node key, and a specific effective key block (EKB) is generated for a group specified by a specific node and distributed thereto so as to limit devices that can be updated. Devices not belonging to the group



cannot be decoded and the distribution security of the keys or the like can be ensured.

LEGAL STATUS

[Date of request for examination] 26.11.2004

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2001-352321

(P2001-352321A)

(43) 公開日 平成13年12月21日 (2001. 12. 21)

(51) Int.Cl. ⁷	識別記号	F I	テームト* (参考)
H 0 4 L 9/08		G 0 6 F 12/14	3 2 0 B 5 B 0 1 7
G 0 6 F 12/14	3 2 0	H 0 4 L 9/00	6 0 1 A 5 J 1 0 4
			6 0 1 D

審査請求 未請求 請求項の数27 O L (全 38 頁)

(21) 出願番号	特願2000-179695(P2000-179695)	(71) 出願人	000002185 ソニー株式会社 東京都品川区北品川6丁目7番35号
(22) 出願日	平成12年6月15日 (2000. 6. 15)	(72) 発明者	石黒 隆二 東京都品川区北品川6丁目7番35号 ソニー株式会社内
(31) 優先権主張番号	特願2000-105329(P2000-105329)	(72) 発明者	大澤 義知 東京都品川区北品川6丁目7番35号 ソニー株式会社内
(32) 優先日	平成12年4月6日 (2000. 4. 6)	(74) 代理人	100101801 弁理士 山田 英治 (外2名)
(33) 優先権主張国	日本 (J P)		

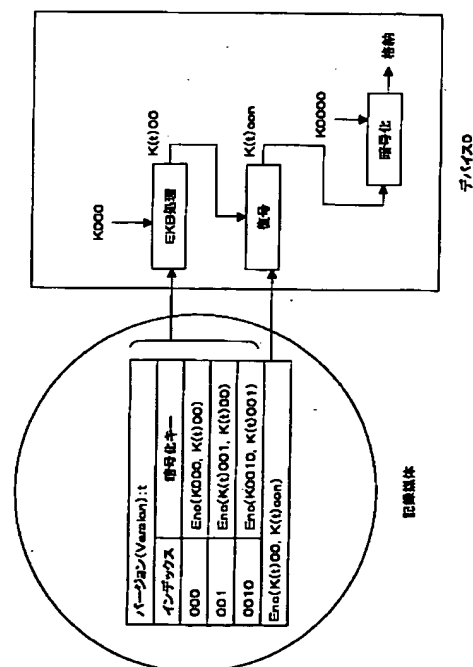
最終頁に続く

(54) 【発明の名称】 情報処理システム、情報処理方法、および情報記録媒体、並びにプログラム提供媒体

(57) 【要約】

【課題】 ツリー（木）構造の暗号化キー構成により各種キーまたはデータの配布を実行して、効率的、安全なデータ配信を可能とした情報処理システムおよび方法を実現する。

【解決手段】 ツリー構造の暗号化鍵構成により、コンテンツキー、認証キー、プログラムデータ等を有効化キーブロック（EKB）とともに送信する。EKBは、ツリーのリーフを構成するデバイスにリーフキーおよび限定したノードキーを保有させた構成であり、特定のノードにより特定されるグループに特定の有効化キーブロック（EKB）を生成して配布して、更新可能デバイスを限定することができる。グループに属さないデバイスは復号できず、キー等の配信安全性が確保される。



【特許請求の範囲】

【請求項1】 1以上の選択されたデバイスにおいてのみ利用可能な暗号化メッセージデータを配信する情報処理システムであり、

個々のデバイスは、

複数の異なるデバイスをリーフとした階層ツリー構造における各ノードに固有のノードキーと各デバイス固有のリーフキーの異なるキーセットをそれぞれ保有するとともに、デバイスに対して配信される前記暗号化メッセージデータについての復号処理を前記キーセットを使用して実行する暗号処理手段を有し、

前記暗号化メッセージデータを配信するメッセージデータ配信手段は、

前記階層ツリー構造の1つのノードを頂点ノードとし、該頂点ノードの下位に連結されるノードおよびリーフによって構成されるグループ内のノードキーの少なくともいずれかを更新した更新ノードキーと、該更新ノードキーを該グループのノードキーあるいはリーフキーによって暗号化した有効化キーブロック（EKB）を生成するとともに、前記更新ノードキーによって暗号化したメッセージデータを生成して配信する構成を有することを特徴とする情報処理システム。

【請求項2】 前記デバイスにおける前記暗号処理手段は、

前記有効化キーブロック（EKB）の処理により、前記更新ノードキーを取得し、該取得した更新ノードキーにより前記暗号化メッセージデータの復号を実行する構成であることを特徴とする請求項1に記載の情報処理システム。

【請求項3】 前記メッセージデータは、コンテンツデータを復号するための復号鍵として使用可能なコンテンツキーであることを特徴とする請求項1に記載の情報処理システム。

【請求項4】 前記メッセージデータは、認証処理において用いられる認証キーであることを特徴とする請求項1に記載の情報処理システム。

【請求項5】 前記メッセージデータは、コンテンツのインテグリティ・チェック値（ICV）生成キーであることを特徴とする請求項1に記載の情報処理システム。

【請求項6】 前記メッセージデータは、認証処理において用いられる認証キーであることを特徴とする請求項1に記載の情報処理システム。

【請求項7】 前記メッセージデータは、プログラムコードであることを特徴とする請求項1に記載の情報処理システム。

【請求項8】 前記メッセージデータ配信手段は、前記有効化キーブロック（EKB）と、前記メッセージデータとしてコンテンツデータを復号するための復号鍵として使用可能なコンテンツキーと、前記コンテンツキーで暗号化した暗号化コンテンツとに

よって構成される暗号化データを配信する構成であることを特徴とする請求項1に記載の情報処理システム。

【請求項9】 前記メッセージデータ配信手段と前記デバイスは、

それぞれ認証処理を実行する認証処理手段を有し、前記メッセージデータの配信は、前記メッセージデータ配信手段と前記デバイス間での認証処理が成立したことを条件として配信する構成であることを特徴とする請求項1に記載の情報処理システム。

【請求項10】 前記メッセージデータ配信手段と前記デバイス間には異なる中間デバイスが介在し、

前記メッセージデータ配信手段は、前記メッセージデータを配信する目的となる目的デバイスにおいてのみ復号可能な有効化キーブロック（EKB）と暗号化メッセージデータを生成して配信する構成を有することを特徴とする請求項1に記載の情報処理システム。

【請求項11】 前記階層ツリー構造は、1つのノードを頂点ノードとし、該頂点ノードの下位に連結されるノードおよびリーフによって構成されるグループによって構成されるカテゴリグループを含み、

該カテゴリグループは、デバイス種類、サービス種類、管理手段種類等の唯一の定義されたカテゴリに属するデバイスの集合として構成されていることを特徴とする請求項1に記載の情報処理システム。

【請求項12】 前記カテゴリグループは、さらに前記階層ツリー構造の下位段に1以上のサブカテゴリを含み、該サブカテゴリグループは、デバイス種類、サービス種類、管理手段種類等の唯一の定義されたサブカテゴリに属するデバイスの集合として構成されていることを特徴とする請求項11に記載の情報処理システム。

【請求項13】 1以上の選択されたデバイスにおいてのみ利用可能な暗号化メッセージデータをメッセージデータ配信手段から配信する情報処理方法であり、

複数の異なるデバイスをリーフとした階層ツリー構造の1つのノードを頂点ノードとし、該頂点ノードの下位に連結されるノードおよびリーフによって構成されるグループ内のノードキーの少なくともいずれかを更新した更新ノードキーと、該更新ノードキーを該グループのノードキーあるいはリーフキーによって暗号化した有効化キーブロック（EKB）を生成するとともに、前記更新ノードキーによって暗号化したメッセージデータを生成してデバイスに対して配信するメッセージデータ配信ステップと、

前記階層ツリー構造における各ノードに固有のノードキーと各デバイス固有のリーフキーの異なるキーセットをそれぞれ保有するデバイスにおいて、前記暗号化メッセージデータについての復号処理を前記キーセットを使用して実行する復号処理ステップと、を有することを特徴とする情報処理方法。

【請求項14】 前記復号処理ステップは、

前記有効化キーブロック（EKB）の処理により、前記更新ノードキーを取得する更新ノードキー取得ステップと、

前記更新ノードキーにより前記暗号化メッセージデータの復号を実行するメッセージデータ復号ステップと、を含むことを特徴とする請求項13に記載の情報処理方法。

【請求項15】前記メッセージデータは、コンテンツデータを復号するための復号鍵として使用可能なコンテンツキーであることを特徴とする請求項13に記載の情報処理方法。

【請求項16】前記メッセージデータは、認証処理において用いられる認証キーであることを特徴とする請求項13に記載の情報処理方法。

【請求項17】前記メッセージデータは、コンテンツのインテグリティ・チェック値（ICV）生成キーであることを特徴とする請求項13に記載の情報処理方法。

【請求項18】前記メッセージデータは、認証処理において用いられる認証キーであることを特徴とする請求項13に記載の情報処理方法。

【請求項19】前記メッセージデータは、プログラムコードであることを特徴とする請求項13に記載の情報処理方法。

【請求項20】前記メッセージデータ配信手段は、前記有効化キーブロック（EKB）と、前記メッセージデータとしてコンテンツデータを復号するための復号鍵として使用可能なコンテンツキーと前記コンテンツキーで暗号化した暗号化コンテンツとによって構成される暗号化データを配信することを特徴とする請求項13に記載の情報処理方法。

【請求項21】前記メッセージデータ配信手段と前記デバイスは、相互間の認証処理を実行し、前記メッセージデータの配信は、前記メッセージデータ配信手段と前記デバイス間での認証処理が成立したことを条件として配信することを特徴とする請求項13に記載の情報処理方法。

【請求項22】前記メッセージデータ配信手段と前記デバイス間には異なる中間デバイスが介在し、前記メッセージデータ配信手段は、前記メッセージデータを配信する目的となる目的デバイスにおいてのみ復号可能な有効化キーブロック（EKB）と暗号化メッセージデータを生成して配信することを特徴とする請求項13に記載の情報処理方法。

【請求項23】データを格納した情報記録媒体であり、複数の異なるデバイスをリーフとした階層ツリー構造の1つのノードを頂点ノードとし、該頂点ノードの下位に連結されるノードおよびリーフによって構成されるグループ内のノードキーの少なくともいずれかを更新した更新ノードキーと、該更新ノードキーを該グループのノー

ドキーあるいはリーフキーによって暗号化した有効化キーブロック（EKB）と、

前記更新ノードキーによって暗号化したメッセージデータと、を格納したことを特徴とする情報記録媒体。

【請求項24】前記メッセージデータはコンテンツの復号に用いるコンテンツキーであり、

前記情報記録媒体は、さらに、前記コンテンツキーによって暗号化された暗号化コンテンツを格納した構成であることを特徴とする請求項23に記載の情報記録媒体。

【請求項25】前記情報記録媒体は、さらに、コンテンツと該コンテンツに対応するコンテンツキーを取得するために使用される有効化キーブロック（EKB）を対応付けた対応付けデータを格納していることを特徴とする請求項24に記載の情報記録媒体。

【請求項26】前記情報記録媒体は、さらに、コンテンツのインテグリティ・チェック値（ICV）データを格納していることを特徴とする請求項23に記載の情報記録媒体。

【請求項27】暗号化コンテンツデータの復号処理をコンピュータ・システム上で実行せしめるコンピュータ・プログラムを提供するプログラム提供媒体であって、前記コンピュータ・プログラムは、

複数の異なるデバイスをリーフとした階層ツリー構造の1つのノードを頂点ノードとし、該頂点ノードの下位に連結されるノードおよびリーフによって構成されるグループ内のノードキーの少なくともいずれかを更新した更新ノードキーと、該更新ノードキーを該グループのノードキーあるいはリーフキーによって暗号化した有効化キーブロック（EKB）の復号処理により、更新ノードキーを取得する更新ノードキー取得ステップと、前記更新ノードキーによる復号処理を実行して、前記暗号化コンテンツの復号キーとして使用するコンテンツキーを取得するステップと、

前記コンテンツキーにより前記暗号化コンテンツの復号を実行するステップと、

を含むことを特徴とするプログラム提供媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、情報処理システム、情報処理方法、および情報記録媒体、並びにプログラム提供媒体に関し、特に、暗号処理を伴うシステムにおける暗号処理鍵を配信するシステムおよび方法に関する。特に、木構造の階層的鍵配信方式を用いることにより、メッセージ量を小さく抑え、例えばコンテンツキー配信、あるいは各種鍵の更新の際のデータ配信の負荷を軽減し、かつデータの安全性を保持することを可能とする情報処理システム、情報処理方法、および情報記録媒体、並びにプログラム提供媒体に関する。

【0002】

【従来の技術】昨今、ゲームプログラム、音声データ、画像データ等、様々なソフトウェアデータ（以下、これらをコンテンツ（Content）と呼ぶ）を、インターネット等のネットワーク、あるいはDVD、CD等の流通可能な記憶媒体を介しての流通が盛んになってきている。これらの流通コンテンツは、ユーザの所有するP.C（Personal Computer）、ゲーム機器によってデータ受信、あるいは記憶媒体の装着がなされて再生されたり、あるいはP.C等のに付属する記録再生機器内の記録デバイス、例えばメモリカード、ハードディスク等に格納されて、格納媒体からの新たな再生により利用される。

【0003】ビデオゲーム機器、P.C等の情報機器には、流通コンテンツをネットワークから受信するため、あるいはDVD、CD等にアクセスするためのインタフェースを有し、さらにコンテンツの再生に必要となる制御手段、プログラム、データのメモリ領域として使用されるRAM、ROM等を有する。

【0004】音楽データ、画像データ、あるいはプログラム等の様々なコンテンツは、再生機器として利用されるゲーム機器、P.C等の情報機器本体からのユーザ指示、あるいは接続された入力手段を介したユーザの指示により記憶媒体から呼び出され、情報機器本体、あるいは接続されたディスプレイ、スピーカ等を通じて再生される。

【0005】ゲームプログラム、音楽データ、画像データ等、多くのソフトウェア・コンテンツは、一般的にその作成者、販売者に頒布権等が保有されている。従って、これらのコンテンツの配布に際しては、一定の利用制限、すなわち、正規ユーザに対してのみ、ソフトウェアの使用を許諾し、許可のない複製等が行われないようにする、すなわちセキュリティを考慮した構成をとるのが一般的となっている。

【0006】ユーザに対する利用制限を実現する1つの手法が、配布コンテンツの暗号化処理である。すなわち、例えばインターネット等を介して暗号化された音声データ、画像データ、ゲームプログラム等の各種コンテンツを配布するとともに、正規ユーザであると確認された者に対してのみ、配布された暗号化コンテンツを復号する手段、すなわち復号鍵を付与する構成である。

【0007】暗号化データは、所定の手続きによる復号化処理によって利用可能な復号データ（平文）に戻すことができる。このような情報の暗号化処理に暗号化鍵を用い、復号化処理に復号化鍵を用いるデータ暗号化、復号化方法は従来からよく知られている。

【0008】暗号化鍵と復号化鍵を用いるデータ暗号化・復号化方法の態様には様々な種類があるが、その1つの例としていわゆる共通鍵暗号化方式と呼ばれている方式がある。共通鍵暗号化方式は、データの暗号化処理に用いる暗号化鍵とデータの復号化に用いる復号化鍵を共通のものとして、正規のユーザにこれら暗号化処理、復号

化に用いる共通鍵を付与して、鍵を持たない不正ユーザによるデータアクセスを排除するものである。この方式の代表的な方式にDES（データ暗号標準：Data encryption standard）がある。

【0009】上述の暗号化処理、復号化に用いられる暗号化鍵、復号化鍵は、例えばあるパスワード等に基づいてハッシュ関数等の一方方向性関数を適用して得ることができる。一方方向性関数とは、その出力から逆に入力を求めるのは非常に困難となる関数である。例えばユーザが決めたパスワードを入力として一方方向性関数を適用して、その出力に基づいて暗号化鍵、復号化鍵を生成するものである。このようにして得られた暗号化鍵、復号化鍵から、逆にそのオリジナルのデータであるパスワードを求めることは実質上不可能となる。

【0010】また、暗号化するときに使用する暗号化鍵による処理と、復号するときに使用する復号化鍵の処理とを異なるアルゴリズムとした方式がいわゆる公開鍵暗号化方式と呼ばれる方式である。公開鍵暗号化方式は、不特定のユーザが使用可能な公開鍵を使用する方法であり、特定個人に対する暗号化文書を、その特定個人が発行した公開鍵を用いて暗号化処理を行なう。公開鍵によって暗号化された文書は、その暗号化処理に使用された公開鍵に対応する秘密鍵によってのみ復号処理が可能となる。秘密鍵は、公開鍵を発行した個人のみが所有するので、その公開鍵によって暗号化された文書は秘密鍵を持つ個人のみが復号することができる。公開鍵暗号化方式の代表的なものにはRSA（Rivest-Shamir-Adleman）暗号がある。このような暗号化方式を利用することにより、暗号化コンテンツを正規ユーザに対してのみ復号可能とするシステムが可能となる。

【0011】

【発明が解決しようとする課題】上記のようなコンテンツ配信システムでは、コンテンツを暗号化してユーザにネットワーク、あるいはDVD、CD等の記録媒体に格納して提供し、暗号化コンテンツを復号するコンテンツキーを正当なユーザにのみ提供する構成が多く採用されている。コンテンツキー自体の不正なコピー等を防ぐためのコンテンツキーを暗号化して正当なユーザに提供し、正当なユーザのみが有する復号キーを用いて暗号化コンテンツキーを復号してコンテンツキーを使用可能とする構成が提案されている。

【0012】正当なユーザであるか否かの判定は、一般には、例えばコンテンツの送信者であるコンテンツプロバイダとユーザデバイス間において、コンテンツ、あるいはコンテンツキーの配信前に認証処理を実行することによって行なう。一般的な認証処理においては、相手の確認を行なうとともに、その通信でのみ有効なセッションキーを生成して、認証が成立した場合に、生成したセッションキーを用いてデータ、例えばコンテンツあるいはコンテンツキーを暗号化して通信を行なう。認証方式

には、共通鍵暗号方式を用いた相互認証と、公開鍵方式を使用した認証方式があるが、共通鍵を使った認証においては、システムワイドで共通な鍵が必要になり、更新処理等の際に不便である。また、公開鍵方式においては、計算負荷が大きくまた必要なメモリ量も大きくなり、各デバイスにこのような処理手段を設けることは望ましい構成とはいえない。

【0013】本発明では、上述のようなデータの送信者、受信者間の相互認証処理に頼ることなく、正当なユーザに対してのみ、安全にデータを送信することを可能とする情報処理システム、情報処理方法、および情報記録媒体、並びにプログラム提供媒体を提供することを目的とする。

【0014】

【課題を解決するための手段】本発明の第1の側面は、1以上の選択されたデバイスにおいてのみ利用可能な暗号化メッセージデータを配信する情報処理システムであり、個々のデバイスは、複数の異なるデバイスをリーフとした階層ツリー構造における各ノードに固有のノードキーと各デバイス固有のリーフキーの異なるキーセットをそれぞれ保有するとともに、デバイスに対して配信される前記暗号化メッセージデータについての復号処理を前記キーセットを使用して実行する暗号処理手段を有し、前記暗号化メッセージデータを配信するメッセージデータ配信手段は、前記階層ツリー構造の1つのノードを頂点ノードとし、該頂点ノードの下位に連結されるノードおよびリーフによって構成されるグループ内のノードキーの少なくともいずれかを更新した更新ノードキーと、該更新ノードキーを該グループのノードキーあるいはリーフキーによって暗号化した有効化キープブロック(EKB)を生成するとともに、前記更新ノードキーによって暗号化したメッセージデータを生成して配信する構成を有することを特徴とする情報処理システムにある。

【0015】さらに、本発明の情報処理システムの一実施態様において、前記デバイスにおける前記暗号処理手段は、前記有効化キープブロック(EKB)の処理により、前記更新ノードキーを取得し、該取得した更新ノードキーにより前記暗号化メッセージデータの復号を実行する構成であることを特徴とする。

【0016】さらに、本発明の情報処理システムの一実施態様において、前記メッセージデータは、コンテンツデータを復号するための復号鍵として使用可能なコンテンツキーであることを特徴とする。

【0017】さらに、本発明の情報処理システムの一実施態様において、前記メッセージデータは、認証処理において用いられる認証キーであることを特徴とする。

【0018】さらに、本発明の情報処理システムの一実施態様において、前記メッセージデータは、コンテンツのインテグリティ・チェック値(ICV)生成キーであ

ることを特徴とする。

【0019】さらに、本発明の情報処理システムの一実施態様において、前記メッセージデータは、認証処理において用いられる認証キーであることを特徴とする。

【0020】さらに、本発明の情報処理システムの一実施態様において、前記メッセージデータは、プログラムコードであることを特徴とする。

【0021】さらに、本発明の情報処理システムの一実施態様において、前記メッセージデータ配信手段は、前記有効化キープブロック(EKB)と、前記メッセージデータとしてコンテンツデータを復号するための復号鍵として使用可能なコンテンツキーと、前記コンテンツキーで暗号化した暗号化コンテンツとによって構成される暗号化データを配信する構成であることを特徴とする。

【0022】さらに、本発明の情報処理システムの一実施態様において、前記メッセージデータ配信手段と前記デバイスは、それぞれ認証処理を実行する認証処理手段を有し、前記メッセージデータの配信は、前記メッセージデータ配信手段と前記デバイス間での認証処理が成立したことを条件として配信する構成であることを特徴とする。

【0023】さらに、本発明の情報処理システムの一実施態様において、前記メッセージデータ配信手段と前記デバイス間には異なる中間デバイスが介在し、前記メッセージデータ配信手段は、前記メッセージデータを配信する目的となる目的デバイスにおいてのみ復号可能な有効化キープブロック(EKB)と暗号化メッセージデータを生成して配信する構成を有することを特徴とする。

【0024】さらに、本発明の情報処理システムの一実施態様において、前記階層ツリー構造は、1つのノードを頂点ノードとし、該頂点ノードの下位に連結されるノードおよびリーフによって構成されるグループによって構成されるカテゴリグループを含み、該カテゴリグループは、デバイス種類、サービス種類、管理手段種類等の唯一の定義されたカテゴリに属するデバイスの集合として構成されていることを特徴とする。

【0025】さらに、本発明の情報処理システムの一実施態様において、前記カテゴリグループは、さらに前記階層ツリー構造の下位段に1以上のサブカテゴリを含み、該サブカテゴリグループは、デバイス種類、サービス種類、管理手段種類等の唯一の定義されたサブカテゴリに属するデバイスの集合として構成されていることを特徴とする。

【0026】さらに、本発明の第2の側面は、1以上の選択されたデバイスにおいてのみ利用可能な暗号化メッセージデータをメッセージデータ配信手段から配信する情報処理方法であり、複数の異なるデバイスをリーフとした階層ツリー構造の1つのノードを頂点ノードとし、該頂点ノードの下位に連結されるノードおよびリーフによって構成されるグループ内のノードキーの少なくとも

いずれかを更新した更新ノードキーと、該更新ノードキーを該グループのノードキーあるいはリーフキーによって暗号化した有効化キープブロック（EKB）を生成するとともに、前記更新ノードキーによって暗号化したメッセージデータを生成してデバイスに対して配信するメッセージデータ配信ステップと、前記階層ツリー構造における各ノードに固有のノードキーと各デバイス固有のリーフキーの異なるキーセットをそれぞれ保有するデバイスにおいて、前記暗号化メッセージデータについての復号処理を前記キーセットを使用して実行する復号処理ステップと、を有することを特徴とする情報処理方法にある。

【0027】さらに、本発明の情報処理方法の一実施態様において、前記復号処理ステップは、前記有効化キープブロック（EKB）の処理により、前記更新ノードキーを取得する更新ノードキー取得ステップと、前記更新ノードキーにより前記暗号化メッセージデータの復号を実行するメッセージデータ復号ステップとを含むことを特徴とする。

【0028】さらに、本発明の情報処理方法の一実施態様において、前記メッセージデータは、コンテンツデータを復号するための復号鍵として使用可能なコンテンツキーであることを特徴とする。

【0029】さらに、本発明の情報処理方法の一実施態様において、前記メッセージデータは、認証処理において用いられる認証キーであることを特徴とする。

【0030】さらに、本発明の情報処理方法の一実施態様において、前記メッセージデータは、コンテンツのインテグリティ・チェック値（ICV）生成キーであることを特徴とする。

【0031】さらに、本発明の情報処理方法の一実施態様において、前記メッセージデータは、認証処理において用いられる認証キーであることを特徴とする。

【0032】さらに、本発明の情報処理方法の一実施態様において、前記メッセージデータは、プログラムコードであることを特徴とする。

【0033】さらに、本発明の情報処理方法の一実施態様において、前記メッセージデータ配信手段は、前記有効化キープブロック（EKB）と、前記メッセージデータとしてコンテンツデータを復号するための復号鍵として使用可能なコンテンツキーと前記コンテンツキーで暗号化した暗号化コンテンツとによって構成される暗号化データを配信することを特徴とする。

【0034】さらに、本発明の情報処理方法の一実施態様において、前記メッセージデータ配信手段と前記デバイスは、相互間の認証処理を実行し、前記メッセージデータの配信は、前記メッセージデータ配信手段と前記デバイス間での認証処理が成立したことを条件として配信することを特徴とする。

【0035】さらに、本発明の情報処理方法の一実施態

様において、前記メッセージデータ配信手段と前記デバイス間には異なる中間デバイスが介在し、前記メッセージデータ配信手段は、前記メッセージデータを配信する目的となる目的デバイスにおいてのみ復号可能な有効化キープブロック（EKB）と暗号化メッセージデータを生成して配信することを特徴とする。

【0036】さらに、本発明の第3の側面は、データを格納した情報記録媒体であり、複数の異なるデバイスをリーフとした階層ツリー構造の1つのノードを頂点ノードとし、該頂点ノードの下位に連結されるノードおよびリーフによって構成されるグループ内のノードキーの少なくともいずれかを更新した更新ノードキーと、該更新ノードキーを該グループのノードキーあるいはリーフキーによって暗号化した有効化キープブロック（EKB）と、前記更新ノードキーによって暗号化したメッセージデータと、を格納したことを特徴とする情報記録媒体にある。

【0037】さらに、本発明の情報記録媒体の一実施態様において、前記メッセージデータはコンテンツの復号に用いるコンテンツキーであり、前記情報記録媒体は、さらに、前記コンテンツキーによって暗号化された暗号化コンテンツを格納した構成であることを特徴とする。

【0038】さらに、本発明の情報記録媒体の一実施態様において、コンテンツと該コンテンツに対応するコンテンツキーを取得するために使用される有効化キープブロック（EKB）を対応付けた対応付けデータを格納していることを特徴とする。

【0039】さらに、本発明の情報記録媒体の一実施態様において、コンテンツのインテグリティ・チェック値（ICV）データを格納していることを特徴とする。

【0040】さらに、本発明の第4の側面は、暗号化コンテンツデータの復号処理をコンピュータ・システム上で実行せしめるコンピュータ・プログラムを提供するプログラム提供媒体であって、前記コンピュータ・プログラムは、複数の異なるデバイスをリーフとした階層ツリー構造の1つのノードを頂点ノードとし、該頂点ノードの下位に連結されるノードおよびリーフによって構成されるグループ内のノードキーの少なくともいずれかを更新した更新ノードキーと、該更新ノードキーを該グループのノードキーあるいはリーフキーによって暗号化した有効化キープブロック（EKB）の復号処理により、更新ノードキーを取得する更新ノードキー取得ステップと、前記更新ノードキーによる復号処理を実行して、前記暗号化コンテンツの復号キーとして使用するコンテンツキーを取得するステップと、前記コンテンツキーにより前記暗号化コンテンツの復号を実行するステップと、を含むことを特徴とするプログラム提供媒体にある。

【0041】

【作用】本発明の構成においては、ツリー（木）構造の階層的構造の暗号化鍵配信構成を用いることにより、キ

一更新に必要な配信メッセージ量を小さく押さえている。すなわち、各機器をn分木の各葉（リーフ）に配置した構成の鍵配信方法を用い、記録媒体もしくは通信回線を介して、コンテンツデータの暗号鍵であるコンテンツキーもしくは認証処理に用いる認証キー、あるいはプログラムコード等を有効化キーブロックとともに配信する構成としている。

【0042】このようにすることにより、正当なデバイスのみが復号可能なデータを安全に配信することが可能となる。

【0043】なお、本発明の第4の側面に係るプログラム提供媒体は、例えば、様々なプログラム・コードを実行可能な汎用コンピュータ・システムに対して、コンピュータ・プログラムをコンピュータ可読な形式で提供する媒体である。媒体は、CDやFD、MOなどの記録媒体、あるいは、ネットワークなどの伝送媒体など、その形態は特に限定されない。

【0044】このようなプログラム提供媒体は、コンピュータ・システム上で所定のコンピュータ・プログラムの機能を実現するための、コンピュータ・プログラムと提供媒体との構造上又は機能上の協働的關係を定義したものである。換言すれば、該提供媒体を介してコンピュータ・プログラムをコンピュータ・システムにインストールすることによって、コンピュータ・システム上では協働的作用が発揮され、本発明の他の側面と同様の作用効果を得ることができるのである。

【0045】本発明のさらに他の目的、特徴や利点は、後述する本発明の実施例や添付する図面に基づくより詳細な説明によって明らかになるであろう。

【0046】

【発明の実施の形態】〔システム概要〕図1に本発明のデータ処理システムが適用可能なコンテンツ配信システム例を示す。コンテンツの配信側10は、コンテンツ受信側20の有する様々なコンテンツ再生可能な機器に対してコンテンツ、あるいはコンテンツキーを暗号化して送信する。受信側20における機器では、受信した暗号化コンテンツ、あるいは暗号化コンテンツキー等を復号してコンテンツあるいはコンテンツキーを取得して、画像データ、音声データの再生、あるいは各種プログラムの実行等を行なう。コンテンツの配信側10とコンテンツ受信側20との間のデータ交換は、インターネット等のネットワークを介して、あるいはDVD、CD等の流通可能な記憶媒体を介して実行される。

【0047】コンテンツの配信側10のデータ配信手段としては、インターネット11、衛星放送12、電話回線13、DVD、CD等のメディア14等があり、一方、コンテンツ受信側20のデバイスとしては、パーソナルコンピュータ（PC）21、ポータブルデバイス（PD）22、携帯電話、PDA（Personal Digital Assistants）等の携帯機器23、DVD、CDプレーヤ

等の記録再生器24、ゲーム端末等の再生専用器25等がある。これらコンテンツ受信側20の各デバイスは、コンテンツ配信側10から提供されたコンテンツをネットワーク等の通信手段あるいは、あるいはメディア30から取得する。

【0048】〔デバイス構成〕図2に、図1に示すコンテンツ受信側20のデバイスの一例として、記録再生装置100の構成ブロック図を示す。記録再生装置100は、入出力I/F（Interface）120、MPEG（Moving Picture Experts Group）コーデック130、A/D、D/Aコンバータ141を備えた入出力I/F（Interface）140、暗号処理手段150、ROM（Read Only Memory）160、CPU（Central Processing Unit）170、メモリ180、記録媒体195のドライブ190を有し、これらはバス110によって相互に接続されている。

【0049】入出力I/F120は、外部から供給される画像、音声、プログラム等の各種コンテンツを構成するデジタル信号を受信し、バス110上に出力するとともに、バス110上のデジタル信号を受信し、外部に出力する。MPEGコーデック130は、バス110を介して供給されるMPEG符号化されたデータを、MPEGデコードし、入出力I/F140に出力するとともに、入出力I/F140から供給されるデジタル信号をMPEGエンコードしてバス110上に出力する。入出力I/F140は、A/D、D/Aコンバータ141を内蔵している。入出力I/F140は、外部から供給されるコンテンツとしてのアナログ信号を受信し、A/D、D/Aコンバータ141でA/D（Analog Digital）変換することで、デジタル信号として、MPEGコーデック130に出力するとともに、MPEGコーデック130からのデジタル信号を、A/D、D/Aコンバータ141でD/A（Digital Analog）変換することで、アナログ信号として、外部に出力する。

【0050】暗号処理手段150は、例えば、1チップのLSI（Large Scale Integrated Circuit）で構成され、バス110を介して供給されるコンテンツとしてのデジタル信号の暗号化、復号処理、あるいは認証処理を実行し、暗号データ、復号データ等をバス110上に出力する構成を持つ。なお、暗号処理手段150は1チップLSIに限らず、各種のソフトウェアまたはハードウェアを組み合わせた構成によって実現することも可能である。ソフトウェア構成による処理手段としての構成については後段で説明する。

【0051】ROM160は、記録再生装置によって処理されるプログラムデータを格納する。CPU170は、ROM160、メモリ180に記憶されたプログラムを実行することで、MPEGコーデック130や暗号処理手段150等を制御する。メモリ180は、例えば、不揮発性メモリで、CPU170が実行するプログ

ラムや、CPU170の動作に必要なデータ、さらにデバイスによって実行される暗号処理に使用されるキーセットを記憶する。キーセットについては後段で説明する。ドライブ190は、デジタルデータを記録再生可能な記録媒体195を駆動することにより、記録媒体195からデジタルデータを読み出し（再生し）、バス110上に出力するとともに、バス110を介して供給されるデジタルデータを、記録媒体195に供給して記録させる。

【0052】記録媒体195は、例えば、DVD、CD等の光ディスク、光磁気ディスク、磁気ディスク、磁気テープ、あるいはRAM等の半導体メモリ等のデジタルデータの記憶可能な媒体であり、本実施の形態では、ドライブ190に対して着脱可能な構成であるとする。但し、記録媒体195は、記録再生装置100に内蔵する構成としてもよい。

【0053】なお、図2に示す暗号処理手段150は、1つのワンチップLSIとして構成してもよく、また、ソフトウェア、ハードウェアを組み合わせた構成によって実現する構成としてもよい。

【0054】[キー配信構成としてのツリー（木）構造について]次に、図1に示すコンテンツ配信側10からコンテンツ受信側20の各デバイスに暗号データを配信する場合における各デバイスにおける暗号処理鍵の保有構成およびデータ配信構成を図3を用いて説明する。

【0055】図3の最下段に示すナンバ0～15がコンテンツ受信側20の個々のデバイスである。すなわち図3に示す階層ツリー（木）構造の各葉（リーフ：leaf）がそれぞれのデバイスに相当する。

【0056】各デバイス0～15は、製造時あるいは出荷時、あるいはその後において、図3に示す階層ツリー（木）構造における、自分のリーフからルートに至るまでのノードに割り当てられた鍵（ノードキー）および各リーフのリーフキーからなるキーセットをメモリに格納する。図3の最下段に示すK0000～K1111が各デバイス0～15にそれぞれ割り当てられたリーフキーであり、最上段のKR（ルートキー）から、最下段から2番目の節（ノード）に記載されたキー：KR～K111をノードキーとする。

【0057】図3に示すツリー構成において、例えばデバイス0はリーフキーK0000と、ノードキー：K000、K00、K0、KRを所有する。デバイス5はK0101、K010、K01、K0、KRを所有する。デバイス15は、K1111、K111、K11、K1、KRを所有する。なお、図3のツリーにはデバイスが0～15の16個のみ記載され、ツリー構造も4段階構成の均衡のとれた左右対称構成として示しているが、さらに多くのデバイスがツリー中に構成され、また、ツリーの各部において異なる段数構成を持つことが可能である。

【0058】また、図3のツリー構造に含まれる各デバイスには、様々な記録媒体、例えば、デバイス埋め込み型あるいはデバイスに着脱自在に構成されたDVD、CD、MD、フラッシュメモリ等を使用する様々なタイプのデバイスが含まれている。さらに、様々なアプリケーションサービスが共存可能である。このような異なるデバイス、異なるアプリケーションの共存構成の上に図3に示すコンテンツあるいは鍵配布構成である階層ツリー構造が適用される。

【0059】これらの様々なデバイス、アプリケーションが共存するシステムにおいて、例えば図3の点線で囲んだ部分、すなわちデバイス0、1、2、3を同一の記録媒体を用いる1つのグループとして設定する。例えば、この点線で囲んだグループ内に含まれるデバイスに対しては、まとめて、共通のコンテンツを暗号化してプロバイダから送付したり、各デバイス共通に使用するコンテンツキーを送付したり、あるいは各デバイスからプロバイダあるいは決済機関等にコンテンツ料金の支払データをやはり暗号化して出力するといった処理が実行される。コンテンツプロバイダ、あるいは決済処理機関等、各デバイスとのデータ送受信を行なう機関は、図3の点線で囲んだ部分、すなわちデバイス0、1、2、3を1つのグループとして一括してデータを送付する処理を実行する。このようなグループは、図3のツリー中に複数存在する。コンテンツプロバイダ、あるいは決済処理機関等、各デバイスとのデータ送受信を行なう機関は、メッセージデータ配信手段として機能する。

【0060】なお、ノードキー、リーフキーは、ある1つの鍵管理センタによって統括して管理してもよいし、各グループに対する様々なデータ送受信を行なうプロバイダ、決済機関等のメッセージデータ配信手段によってグループごとに管理する構成としてもよい。これらのノードキー、リーフキーは例えばキーの漏洩等の場合に更新処理が実行され、この更新処理は鍵管理センタ、プロバイダ、決済機関等が実行する。

【0061】このツリー構成において、図3から明らかなように、1つのグループに含まれる3つのデバイス0、1、2、3はノードキーとして共通のキーK00、K0、KRを保有する。このノードキー共有構成を利用することにより、例えば共通のコンテンツキーをデバイス0、1、2、3のみに提供することが可能となる。たとえば、共通に保有するノードキーK00自体をコンテンツキーとして設定すれば、新たな鍵送付を実行することなくデバイス0、1、2、3のみが共通のコンテンツキーの設定が可能である。また、新たなコンテンツキーKconをノードキーK00で暗号化した値Enc（K00、Kcon）を、ネットワークを介してあるいは記録媒体に格納してデバイス0、1、2、3に配布すれば、デバイス0、1、2、3のみが、それぞれのデバイスにおいて保有する共有ノードキーK00を用いて暗号

Enc (K00, Kcon) を解いてコンテンツキー: Kcon を得ることが可能となる。なお、Enc (Ka, Kb) は Kb を Ka によって暗号化したデータであることを示す。

【0062】また、ある時点 t において、デバイス 3 の所有する鍵: K0011, K001, K00, K0, KR が攻撃者 (ハッカー) により解析されて露呈したことが発覚した場合、それ以降、システム (デバイス 0, 1, 2, 3 のグループ) で送受信されるデータを守るために、デバイス 3 をシステムから切り離す必要がある。そのためには、ノードキー: K001, K00, K0, KR をそれぞれ新たな鍵 K(t)001, K(t)00, K(t)0, K(t)R に更新し、デバイス 0, 1, 2 にその更新キーを伝える必要がある。ここで、K(t)aaa は、鍵 Kaaa の世代 (Generation): t の更新キーであることを示す。

【0063】更新キーの配布処理について説明する。キーの更新は、例えば、図 4 (A) に示す有効化キーブロック (EKB: Enabling Key Block) と呼ばれるブロックデータによって構成されるテーブルをたとえばネットワーク、あるいは記録媒体に格納してデバイス 0, 1, 2 に供給することによって実行される。なお、有効化キーブロック (EKB) は、図 3 に示すようなツリー構造を構成する各リーフに対応するデバイスに新たに更新されたキーを配布するための暗号化キーによって構成される。有効化キーブロック (EKB) は、キー更新ブロック (KRB: KeyRenewal Block) と呼ばれることもある。

【0064】図 4 (A) に示す有効化キーブロック (EKB) には、ノードキーの更新に必要なデバイスのみが更新可能なデータ構成を持つブロックデータとして構成される。図 4 の例は、図 3 に示すツリー構造中のデバイス 0, 1, 2 において、世代 t の更新ノードキーを配布することを目的として形成されたブロックデータである。図 3 から明かなように、デバイス 0, デバイス 1 は、更新ノードキーとして K(t)00, K(t)0, K(t)R が必要であり、デバイス 2 は、更新ノードキーとして K(t)001, K(t)00, K(t)0, K(t)R が必要である。

【0065】図 4 (A) の EKB に示されるように EKB には複数の暗号化キーが含まれる。最下段の暗号化キーは、Enc (K0010, K(t)001) である。これはデバイス 2 の持つリーフキー K0010 によって暗号化された更新ノードキー K(t)001 であり、デバイス 2 は、自身の持つリーフキーによってこの暗号化キーを復号し、K(t)001 を得ることができる。また、復号により得た K(t)001 を用いて、図 4

(A) の下から 2 段目の暗号化キー Enc (K(t)001, K(t)00) を復号可能となり、更新ノードキー K(t)00 を得ることができる。以下順次、図 4

(A) の上から 2 段目の暗号化キー Enc (K(t)00, K(t)0) を復号し、更新ノードキー K(t)0、図 4 (A) の上から 1 段目の暗号化キー Enc (K(t)0, K(t)R) を復号し K(t)R を得る。一方、デバイス K0000, K0001 は、ノードキー K000 は更新する対象に含まれておらず、更新ノードキーとして必要なのは、K(t)00, K(t)0, K(t)R である。デバイス K0000, K0001 は、図 4 (A) の上から 3 段目の暗号化キー Enc (K000, K(t)00) を復号し K(t)00 を取得し、以下、図 4 (A) の上から 2 段目の暗号化キー Enc (K(t)00, K(t)0) を復号し、更新ノードキー K(t)0、図 4 (A) の上から 1 段目の暗号化キー Enc (K(t)0, K(t)R) を復号し K(t)R を得る。このようにして、デバイス 0, 1, 2 は更新した鍵 K(t)001, K(t)00, K(t)0, K(t)R を得ることができる。なお、図 4 (A) のインデックスは、復号キーとして使用するノードキー、リーフキーの絶対番地を示す。

【0066】図 3 に示すツリー構造の上位段のノードキー: K(t)0, K(t)R の更新が不要であり、ノードキー K00 のみの更新処理が必要である場合には、図 4 (B) の有効化キーブロック (EKB) を用いることで、更新ノードキー K(t)00 をデバイス 0, 1, 2 に配布することができる。

【0067】図 4 (B) に示す EKB は、例えば特定のグループにおいて共有する新たなコンテンツキーを配布する場合に利用可能である。具体例として、図 3 に点線で示すグループ内のデバイス 0, 1, 2, 3 がある記録媒体を用いており、新たな共通のコンテンツキー K(t)con が必要であるとする。このとき、デバイス 0, 1, 2, 3 の共通のノードキー K00 を更新した K(t)00 を用いて新たな共通の更新コンテンツキー: K(t)con を暗号化したデータ Enc (K(t), K(t)con) を図 4 (B) に示す EKB とともに配布する。この配布により、デバイス 4 など、その他のグループの機器においては復号されないデータとしての配布が可能となる。

【0068】すなわち、デバイス 0, 1, 2 は EKB を処理して得た K(t)00 を用いて上記暗号文を復号すれば、t 時点でのコンテンツキー K(t)con を得ることが可能になる。

【0069】[EKB を使用したコンテンツキーの配布] 図 5 に、t 時点でのコンテンツキー K(t)con を得る処理例として、K(t)00 を用いて新たな共通のコンテンツキー K(t)con を暗号化したデータ Enc (K(t)00, K(t)con) と図 4 (B) に示す EKB とを記録媒体を介して受領したデバイス 0 の処理を示す。すなわち EKB による暗号化メッセージデータをコンテンツキー K(t)con とした例である。

【0070】図5に示すように、デバイス0は、記録媒体に格納されている世代：t時点のEKBと自分がかじめ格納しているノードキーK000を用いて上述したと同様のEKB処理により、ノードキーK(t)00を生成する。さらに、復号した更新ノードキーK(t)00を用いて更新コンテンツキーK(t)conを復号して、後にそれを使用するために自分だけが持つリーフキーK0000で暗号化して格納する。

【0071】[EKBのフォーマット] 図6に有効化キーブロック(EKB)のフォーマット例を示す。バージョン601は、有効化キーブロック(EKB)のバージョンを示す識別子である。なお、バージョンは最新のEKBを識別する機能とコンテンツとの対応関係を示す機能を持つ。デプスは、有効化キーブロック(EKB)の配布先のデバイスに対する階層ツリーの階層数を示す。データポインタ603は、有効化キーブロック(EKB)中のデータ部の位置を示すポインタであり、タグポインタ604はタグ部の位置、署名ポインタ605は署名の位置を示すポインタである。

【0072】データ部606は、例えば更新するノードキーを暗号化したデータを格納する。例えば図5に示すような更新されたノードキーに関する各暗号化キー等を格納する。

【0073】タグ部607は、データ部に格納された暗号化されたノードキー、リーフキーの位置関係を示すタグである。このタグの付与ルールを図7を用いて説明する。図7では、データとして先に図4(A)で説明した有効化キーブロック(EKB)を送付する例を示している。この時のデータは、図7の表(b)に示すようになる。このときの暗号化キーに含まれるトップノードのアドレスをトップノードアドレスとする。この場合は、ルートキーの更新キーK(t)Rが含まれているので、トップノードアドレスはKRとなる。このとき、例えば最上段のデータEnc(K(t)0, K(t)R)は、図7の(a)に示す階層ツリーに示す位置にある。ここで、次のデータは、Enc(K(t)00, K(t)0)であり、ツリー上では前のデータの左下の位置にある。データがある場合は、タグが0、ない場合は1が設定される。タグは、[左(L)タグ、右(R)タグ]として設定される。最上段のデータEnc(K(t)0, K(t)R)の左にはデータがあるので、Lタグ=0、右にはデータがないので、Rタグ=1となる。以下、すべてのデータにタグが設定され、図7(c)に示すデータ列、およびタグ列が構成される。

【0074】タグは、データEnc(Kxxx, Kyyy)がツリー構造のどこに位置しているのかを示すために設定されるものである。データ部に格納されるキーデータEnc(Kxxx, Kyyy)...は、単純に暗号化されたキーの羅列データに過ぎないので、上述したタグによってデータとして格納された暗号化キーのツリー

上の位置を判別可能としたものである。上述したタグを用いずに、先の図4で説明した構成のように暗号化データに対応させたノード・インデックスを用いて、例えば、

0: Enc(K(t)0, K(t)root)
00: Enc(K(t)00, K(t)0)
000: Enc(K(t)000, K(T)00)

...のようなデータ構成とすることも可能であるが、このようなインデックスを用いた構成とすると冗長なデータとなりデータ量が増大し、ネットワークを介する配信等においては好ましくない。これに対し、上述したタグをキー位置を示す索引データとして用いることにより、少ないデータ量でキー位置の判別が可能となる。

【0075】図6に戻って、EKBフォーマットについてさらに説明する。署名(Signature)は、有効化キーブロック(EKB)を発行した例えば鍵管理センタ、コンテンツプロバイダ、決済機関等が実行する電子署名である。EKBを受領したデバイスは署名検証によって正当な有効化キーブロック(EKB)発行者が発行した有効化キーブロック(EKB)であることを確認する。

【0076】[EKBを使用したコンテンツキーおよびコンテンツの配信] 上述の例では、コンテンツキーのみをEKBとともに送付する例について説明したが、コンテンツキーで暗号化したコンテンツと、コンテンツキー暗号キーで暗号化したコンテンツキーと、EKBによって暗号化したコンテンツキー暗号鍵を併せて送付する構成について以下説明する。

【0077】図8にこのデータ構成を示す。図8(a)に示す構成において、Enc(Kcon, content)801は、コンテンツ(Content)をコンテンツキー(Kcon)で暗号化したデータであり、Enc(KEK, Kcon)802は、コンテンツキー(Kcon)をコンテンツキー暗号キー(KEK: Key Encryption Key)で暗号化したデータであり、Enc(EKB, KEK)803は、コンテンツキー暗号キーKEKを有効化キーブロック(EKB)によって暗号化したデータであることを示す。

【0078】ここで、コンテンツキー暗号キーKEKは、図3で示すノードキー(K000, K00...)、あるいはルートキー(KR)自体であってもよく、またノードキー(K000, K00...)、あるいはルートキー(KR)によって暗号化されたキーであってもよい。

【0079】図8(b)は、複数のコンテンツがメディアに記録され、それぞれが同じEnc(EKB, KEK)805を利用している場合の構成例を示す、このような構成においては、各データに同じEnc(EKB, KEK)を付加することなく、Enc(EKB, KEK)にリンクするリンク先を示すデータを各データに付加する構成とすることができる。

【0080】図9にコンテンツキー暗号キーKEKを、

図3に示すノードキーK00を更新した更新ノードキーK(t)00として構成した場合の例を示す。この場合、図3の点線枠で囲んだグループにおいてデバイス3が、例えば鍵の漏洩によりリボーク（排除）されているとして、他のグループのメンバ、すなわち、デバイス0, 1, 2に対して図9に示す(a)有効化キーブロック(EKB)と、(b)コンテンツキー(Kcon)をコンテンツキー暗号キー(KEK=K(t)00)で暗号化したデータと、(c)コンテンツ(content)をコンテンツキー(Kcon)で暗号化したデータとを配信することにより、デバイス0, 1, 2はコンテンツを得ることができる。

【0081】図9の右側には、デバイス0における復号手順を示してある。デバイス0は、まず、受領した有効化キーブロックから自身の保有するリーフキーK000を用いた復号処理により、コンテンツキー暗号キー(KEK=K(t)00)を取得する。次に、K(t)00による復号によりコンテンツキーKconを取得し、さらにコンテンツキーKconによりコンテンツの復号を行なう。これらの処理により、デバイス0はコンテンツを利用可能となる。デバイス1, 2においても各々異なる処理手順でEKBを処理することにより、コンテンツキー暗号キー(KEK=K(t)00)を取得することが可能となり、同様にコンテンツを利用することが可能となる。

【0082】図3に示す他のグループのデバイス4, 5, 6…は、この同様のデータ(EKB)を受信したとしても、自身の保有するリーフキー、ノードキーを用いてコンテンツキー暗号キー(KEK=K(t)00)を取得することができない。同様にリボークされたデバイス3においても、自身の保有するリーフキー、ノードキーでは、コンテンツキー暗号キー(KEK=K(t)00)を取得することができず、正当な権利を有するデバイスのみがコンテンツを復号して利用することが可能となる。

【0083】このように、EKBを利用したコンテンツキーの配送を用いれば、データ量を少なくして、かつ安全に正当権利者のみが復号可能とした暗号化コンテンツを配信することが可能となる。

【0084】なお、有効化キーブロック(EKB)、コンテンツキー、暗号化コンテンツ等は、ネットワークを介して安全に配信することが可能な構成であるが、有効化キーブロック(EKB)、コンテンツキー、暗号化コンテンツをDVD、CD等の記録媒体に格納してユーザに提供することも可能である。この場合、記録媒体に格納された暗号化コンテンツの復号には、同一の記録媒体に格納された有効化キーブロック(EKB)の復号により得られるコンテンツキーを使用するように構成すれば、予め正当権利者のみが保有するリーフキー、ノードキーによってのみ利用可能な暗号化コンテンツの配布処

理、すなわち利用可能なユーザデバイスを限定したコンテンツ配布が簡易な構成で実現可能となる。

【0085】図10に記録媒体に暗号化コンテンツとともに有効化キーブロック(EKB)を格納した構成例を示す。図10に示す例においては、記録媒体にコンテンツC1~C4が格納され、さらに各格納コンテンツに対応する有効化キーブロック(EKB)を対応付けたデータが格納され、さらにバージョンMの有効化キーブロック(EKB_M)が格納されている。例えばEKB_1はコンテンツC1を暗号化したコンテンツキーKcon1を生成するのに使用され、例えばEKB_2はコンテンツC2を暗号化したコンテンツキーKcon2を生成するのに使用される。この例では、バージョンMの有効化キーブロック(EKB_M)が記録媒体に格納されており、コンテンツC3, C4は有効化キーブロック

(EKB_M)に対応付けられているので、有効化キーブロック(EKB_M)の復号によりコンテンツC3, C4のコンテンツキーを取得することができる。EKB_1, EKB_2はディスクに格納されていないので、新たな提供手段、例えばネットワーク配信、あるいは記録媒体による配信によってそれぞれのコンテンツキーを復号するために必要なEKB_1, EKB_2を取得することが必要となる。

【0086】図11に、複数のデバイス間でコンテンツキーが流通する場合のEKBを利用したコンテンツキーの配信と、従来のコンテンツキー配信処理の比較例を示す。上段(a)従来構成であり、下段(b)が本発明の有効化キーブロック(EKB)を利用した例である。なお、図11においてKa(Kb)は、KbをKaで暗号化したデータであることを示す。

【0087】(a)に示すように、従来は、データ送受信者の正当性を確認し、またデータ送信の暗号化処理に使用するセッションキーKsesを共有するために各デバイス間において、認証処理および鍵交換処理(AKE: Authentication and Key Exchange)を実行し、認証が成立したことを条件としてセッションキーKsesでコンテンツキーKconを暗号化して送信する処理を行っていた。

【0088】例えば図11(a)のPCにおいては、受信したセッションキーで暗号化したコンテンツキーKses(Kcon)をセッションキーで復号してKconを得ることが可能であり、さらに取得したKconをPC自体の保有する保存キーKstrで暗号化して自身のメモリに保存することが可能となる。

【0089】図11(a)において、コンテンツプロバイダは、図11(a)の記録デバイス1101にのみデータを利用可能な形で配信したい場合でも、間にPC、再生装置が存在する場合は、図11(a)に示すように認証処理を実行し、それぞれのセッションキーでコンテンツキーを暗号化して配信するといった処理が必要とな

る。また、間に介在するPC、再生装置においても認証処理において生成し共有することになったセッションキーを用いることで暗号化コンテンツキーを復号してコンテンツキーを取得可能となる。

【0090】一方、図11(b)の下段に示す有効化キーブロック(EKB)を利用した例においては、コンテンツプロバイダから有効化キーブロック(EKB)と、有効化キーブロック(EKB)の処理によって得られるノードキー、またはルートキーによってコンテンツキーKconを暗号化したデータ(図の例ではKroot(Kcon))を配信することにより、配信したEKBの処理が可能な機器においてのみコンテンツキーKconを復号して取得することが可能になる。

【0091】従って、例えば図11(b)の右端にのみ利用可能な有効化キーブロック(EKB)を生成して、その有効化キーブロック(EKB)と、そのEKB処理によって得られるノードキー、またはルートキーによってコンテンツキーKconを暗号化したデータを併せて送ることにより、間に存在するPC、再生機器等は、自身の有するリーフキー、ノードキーによっては、EKBの処理を実行することができない。従って、データ送受信デバイス間での認証処理、セッションキーの生成、セッションキーによるコンテンツキーKconの暗号化処理といった処理を実行することなく、安全に正当なデバイスに対してのみ利用可能なコンテンツキーを配信することが可能となる。

【0092】PC、記録再生器にも利用可能なコンテンツキーを配信したい場合は、それぞれにおいて処理可能な有効化キーブロック(EKB)を生成して、配信することにより、共通のコンテンツキーを取得することが可能となる。

【0093】[有効化キーブロック(EKB)を使用した認証キーの配信(共通鍵方式)] 上述の有効化キーブロック(EKB)を使用したデータあるいはキーの配信において、デバイス間で転送される有効化キーブロック(EKB)およびコンテンツあるいはコンテンツキーは常に同じ暗号化形態を維持しているため、データ伝走路を盗み出して記録し、再度、後で転送する、いわゆるリプレイアタックにより、不正コピーが生成される可能性がある。これを防ぐ構成としては、データ転送デバイス間において、従来と同様の認証処理および鍵交換処理を実行することが有効な手段である。ここでは、この認証処理および鍵交換処理を実行する際に使用する認証キーKakeを上述の有効化キーブロック(EKB)を使用してデバイスに配信することにより、安全な秘密鍵として共有する認証キーを持ち、共通鍵方式に従った認証処理を実行する構成について説明する。すなわちEKBによる暗号化メッセージデータを認証キーとした例である。

【0094】図12に、共通鍵暗号方式を用いた相互認

証方法(ISO/IEC 9798-2)を示す。図12においては、共通鍵暗号方式としてDESを用いているが、共通鍵暗号方式であれば他の方式も可能である。図12において、まず、Bが64ビットの乱数Rbを生成し、Rbおよび自己のIDであるID(b)をAに送信する。これを受信したAは、新たに64ビットの乱数Raを生成し、Ra、Rb、ID(b)の順に、DESのCBCモードで鍵Kabを用いてデータを暗号化し、Bに返送する。なお、鍵Kabは、AおよびBに共通の秘密鍵としてそれぞれの記録素子内に格納する鍵である。DESのCBCモードを用いた鍵Kabによる暗号化処理は、例えばDESを用いた処理においては、初期値とRaとを排他的論理和し、DES暗号化部において、鍵Kabを用いて暗号化し、暗号文E1を生成し、続けて暗号文E1とRbとを排他的論理和し、DES暗号化部において、鍵Kabを用いて暗号化し、暗号文E2を生成し、さらに、暗号文E2とID(b)とを排他的論理和し、DES暗号化部において、鍵Kabを用いて暗号化して生成した暗号文E3とによって送信データ(Token-AB)を生成する。

【0095】これを受信したBは、受信データを、やはり共通の秘密鍵としてそれぞれの記録素子内に格納する鍵Kab(認証キー)で復号化する。受信データの復号化方法は、まず、暗号文E1を認証キーKabで復号化し、乱数Raを得る。次に、暗号文E2を認証キーKabで復号化し、その結果とE1を排他的論理和し、Rbを得る。最後に、暗号文E3を認証キーKabで復号化し、その結果とE2を排他的論理和し、ID(b)を得る。こうして得られたRa、Rb、ID(b)のうち、RbおよびID(b)が、Bが送信したものと一致するか検証する。この検証に通った場合、BはAを正当なものとして認証する。

【0096】次にBは、認証後に使用するセッションキー(Kses)を生成する(生成方法は、乱数を用いる)。そして、Rb、Ra、Ksesの順に、DESのCBCモードで認証キーKabを用いて暗号化し、Aに返送する。

【0097】これを受信したAは、受信データを認証キーKabで復号化する。受信データの復号化方法は、Bの復号化処理と同様であるので、ここでは詳細を省略する。こうして得られたRb、Ra、Ksesの内、RbおよびRaが、Aが送信したものと一致するか検証する。この検証に通った場合、AはBを正当なものとして認証する。互いに相手を認証した後は、セッションキーKsesは、認証後の秘密通信のための共通鍵として利用される。

【0098】なお、受信データの検証の際に、不正、不一致が見つかった場合には、相互認証が失敗したものとして処理を中断する。

【0099】上述の認証処理においては、A、Bは共通

の認証キー K_{ab} を共有する。この共通鍵 K_{ab} を上述の有効化キープロック (EKB) を使用してデバイスに配信する。

【0100】例えば、図12の例では、A、またはBのいずれかが他方が復号可能な有効化キープロック (EKB) を生成して生成した有効化キープロック (EKB) によって認証キー K_{ab} を暗号化して、他方に送信する構成としてもよいし、あるいは第3者がデバイスA、Bに対して双方が利用可能な有効化キープロック (EKB) を生成してデバイスA、Bに対して生成した有効化キープロック (EKB) によって認証キー K_{ab} を暗号化して配信する構成としてもよい。

【0101】図13および図14に複数のデバイスに共通の認証キー K_{ake} を有効化キープロック (EKB) によって配信する構成例を示す。図13はデバイス0、1、2、3に対して復号可能な認証キー K_{ake} を配信する例、図14はデバイス0、1、2、3中のデバイス3をリボーク (排除) してデバイス0、1、2に対してのみ復号可能な認証キーを配信する例を示す。

【0102】図13の例では、更新ノードキー $K(t)00$ によって、認証キー K_{ake} を暗号化したデータ(b)とともに、デバイス0、1、2、3においてそれぞれの有するノードキー、リーフキーを用いて更新されたノードキー $K(t)00$ を復号可能な有効化キープロック (EKB) を生成して配信する。それぞれのデバイスは、図13の右側に示すようにまず、EKBを処理 (復号) することにより、更新されたノードキー $K(t)00$ を取得し、次に、取得したノードキー $K(t)00$ を用いて暗号化された認証キー $Enc(K(t)00, K_{ake})$ を復号して認証キー K_{ake} を得ることが可能となる。

【0103】その他のデバイス4、5、6、7…は同一の有効化キープロック (EKB) を受信しても自身の保有するノードキー、リーフキーでは、EKBを処理して更新されたノードキー $K(t)00$ を取得することができないので、安全に正当なデバイスに対してのみ認証キーを送付することができる。

【0104】一方、図14の例は、図3の点線枠で囲んだグループにおいてデバイス3が、例えば鍵の漏洩によりリボーク (排除) されているとして、他のグループのメンバ、すなわち、デバイス0、1、2、に対してのみ復号可能な有効化キープロック (EKB) を生成して配信した例である。図14に示す(a)有効化キープロック (EKB) と、(b) 認証キー (K_{ake}) をノードキー ($K(t)00$) で暗号化したデータを配信する。

【0105】図14の右側には、復号手順を示してある。デバイス0、1、2は、まず、受領した有効化キープロックから自身の保有するリーフキーまたはノードキーを用いた復号処理により、更新ノードキー ($K(t)00$) を取得する。次に、 $K(t)00$ による復号によ

り認証キー K_{ake} を取得する。

【0106】図3に示す他のグループのデバイス4、5、6…は、この同様のデータ (EKB) を受信したとしても、自身の保有するリーフキー、ノードキーを用いて更新ノードキー ($K(t)00$) を取得することができない。同様にリボークされたデバイス3においても、自身の保有するリーフキー、ノードキーでは、更新ノードキー ($K(t)00$) を取得することができず、正当な権利を有するデバイスのみが認証キーを復号して利用することが可能となる。

【0107】このように、EKBを利用した認証キーの配送を用いれば、データ量を少なくして、かつ安全に正当権利者のみが復号可能とした認証キーを配信することが可能となる。

【0108】[公開鍵認証と有効化キープロック (EKB) を使用したコンテンツキーの配信] 次に、公開鍵認証と有効化キープロック (EKB) を使用したコンテンツキーの配信処理について説明する。まず、公開鍵暗号方式である160ビット長の楕円曲線暗号を用いた相互認証方法を、図15を用いて説明する。図15において、公開鍵暗号方式としてECCを用いているが、同様な公開鍵暗号方式であればいずれでもよい。また、鍵サイズも160ビットでなくてもよい。図15において、まずBが、64ビットの乱数 R_b を生成し、Aに送信する。これを受信したAは、新たに64ビットの乱数 R_a および素数 p より小さい乱数 A_k を生成する。そして、ベースポイント G を A_k 倍した点 $A_v = A_k \times G$ を求め、 R_a 、 R_b 、 A_v (X座標とY座標) に対する電子署名 $A.Sig$ を生成し、Aの公開鍵証明書とともにBに返送する。ここで、 R_a および R_b はそれぞれ64ビット、 A_v のX座標とY座標がそれぞれ160ビットであるので、合計448ビットに対する電子署名を生成する。

【0109】Aの公開鍵証明書、 R_a 、 R_b 、 A_v 、電子署名 $A.Sig$ を受信したBは、Aが送信してきた R_b が、Bが生成したものと一致するか検証する。その結果、一致していた場合には、Aの公開鍵証明書内の電子署名を認証局の公開鍵で検証し、Aの公開鍵を取り出す。そして、取り出したAの公開鍵を用い電子署名 $A.Sig$ を検証する。

【0110】次に、Bは、素数 p より小さい乱数 B_k を生成する。そして、ベースポイント G を B_k 倍した点 $B_v = B_k \times G$ を求め、 R_b 、 R_a 、 B_v (X座標とY座標) に対する電子署名 $B.Sig$ を生成し、Bの公開鍵証明書とともにAに返送する。

【0111】Bの公開鍵証明書、 R_b 、 R_a 、 A_v 、電子署名 $B.Sig$ を受信したAは、Bが送信してきた R_a が、Aが生成したものと一致するか検証する。その結果、一致していた場合には、Bの公開鍵証明書内の電子署名を認証局の公開鍵で検証し、Bの公開鍵を取り出

す。そして、取り出したBの公開鍵を用い電子署名B・Sigを検証する。電子署名の検証に成功した後、AはBを正当なものとして認証する。

【0112】両者が認証に成功した場合には、Bは $B_k \times A_v$ (B_k は乱数だが、 A_v は楕円曲線上の点であるため、楕円曲線上の点のスカラー倍計算が必要)を計算し、Aは $A_k \times B_v$ を計算し、これら点のX座標の下位64ビットをセッションキーとして以降の通信に使用する(共通鍵暗号を64ビット鍵長の共通鍵暗号とした場合)。もちろん、Y座標からセッション鍵を生成してもよいし、下位64ビットでなくてもよい。なお、相互認証後の秘密通信においては、送信データはセッションキーで暗号化されるだけでなく、電子署名も付されることがある。

【0113】電子署名の検証や受信データの検証の際に、不正、不一致が見つかった場合には、相互認証が失敗したものとして処理を中断する。

【0114】図16に公開鍵認証と有効化キーブロック(EKB)を使用したコンテンツキーの配信処理例を示す。まずコンテンツプロバイダとPC間において図15で説明した公開鍵方式による認証処理が実行される。コンテンツプロバイダは、コンテンツキー配信先である再生装置、記録媒体の有するノードキー、リーフキーによって復号可能なEKBを生成して、更新ノードキーによる暗号化を実行したコンテンツキーE(Kcon)と、有効化キーブロック(EKB)とをPC間の認証処理において生成したセッションキーKsesで暗号化してPCに送信する。

【0115】PCはセッションキーで暗号化された[更新ノードキーによる暗号化を実行したコンテンツキーE(Kcon)と、有効化キーブロック(EKB)]をセッションキーで復号した後、再生装置、記録媒体に送信する。

【0116】再生装置、記録媒体は、自身の保有するノードキーまたはリーフキーによって[更新ノードキーによる暗号化を実行したコンテンツキーE(Kcon)と、有効化キーブロック(EKB)]を復号することによってコンテンツキーKconを取得する。

【0117】この構成によれば、コンテンツプロバイダとPC間での認証を条件として[更新ノードキーによる暗号化を実行したコンテンツキーE(Kcon)と、有効化キーブロック(EKB)]が送信されるので、例えば、ノードキーの漏洩があった場合でも、確実な相手に対するデータ送信が可能となる。

【0118】[プログラムコードの有効化キーブロック(EKB)を使用した配信] 上述した例では、コンテンツキー、認証キー等を有効化キーブロック(EKB)を用いて暗号化して配信する方法を説明したが、様々なプログラムコードを有効化キーブロック(EKB)を用いて配信する構成も可能である。すなわちEKBによる暗

号化メッセージデータをプログラムコードとした例である。以下、この構成について説明する。

【0119】図17にプログラムコードを有効化キーブロック(EKB)の例えば更新ノードキーによって暗号化してデバイス間で送信する例を示す。デバイス1701は、デバイス1702の有するノードキー、リーフキーによって復号可能な有効化キーブロック(EKB)と、有効化キーブロック(EKB)に含まれる更新ノードキーで暗号処理したプログラムコードをデバイス1702に送信する。デバイス1702は受信したEKBを処理して更新ノードキーを取得して、さらに取得した更新ノードキーによってプログラムコードの復号を実行して、プログラムコードを得る。

【0120】図17に示す例では、さらに、デバイス1702において取得したプログラムコードによる処理を実行して、その結果をデバイス1701に返して、デバイス1701がその結果に基づいて、さらに処理を続行する例を示している。

【0121】このように有効化キーブロック(EKB)と、有効化キーブロック(EKB)に含まれる更新ノードキーで暗号処理したプログラムコードを配信することにより、特定のデバイスにおいて解読可能なプログラムコードを前述の図3で示した特定のデバイス、あるいはグループに対して配信することが可能となる。

【0122】[送信コンテンツに対するチェック値(ICV: Integrity Check Value)を対応させる構成] 次に、コンテンツの改竄を防止するためにコンテンツのインテグリティ・チェック値(ICV)を生成して、コンテンツに対応付けて、ICVの計算により、コンテンツ改竄の有無を判定する処理構成について説明する。

【0123】コンテンツのインテグリティ・チェック値(ICV)は、例えばコンテンツに対するハッシュ関数を用いて計算され、 $ICV = hash(Kicv, C1, C2, \dots)$ によって計算される。 $Kicv$ はICV生成キーである。 $C1, C2$ はコンテンツの情報であり、コンテンツの重要情報のメッセージ認証符号(MAC: Message authentication Code)が使用される。

【0124】DES暗号処理構成を用いたMAC値生成例を図18に示す。図18の構成に示すように対象となるメッセージを8バイト単位に分割し、(以下、分割されたメッセージをM1、M2、・・・、MNとする)、まず、初期値(Initial Value (以下、IVとする))とM1を排他的論理和する(その結果をI1とする)。次に、I1をDES暗号化部に入れ、鍵(以下、K1とする)を用いて暗号化する(出力をE1とする)。続けて、E1およびM2を排他的論理和し、その出力I2をDES暗号化部へ入れ、鍵K1を用いて暗号化する(出力E2)。以下、これを繰り返す、全てのメッセージに対して暗号化処理を施す。最後に出てきたENがメッセージ認証符号(MAC (Message Authentication Cod

e)) となる。

【0125】このようなコンテンツのMAC値とICV生成キーにハッシュ関数を適用して用いてコンテンツのインテグリティ・チェック値(ICV)が生成される。改竄のないことが保証された例えばコンテンツ生成時に生成したICVと、新たにコンテンツに基づいて生成したICVとを比較して同一のICVが得られればコンテンツに改竄のないことが保証され、ICVが異なれば、改竄があったと判定される。

【0126】[チェック値(ICV)の生成キーKicvをEKBによって配布する構成]次に、コンテンツのインテグリティ・チェック値(ICV)生成キーであるKicvを上記の有効化キープブロックによって送付する構成について説明する。すなわちEKBによる暗号化メッセージデータをコンテンツのインテグリティ・チェック値(ICV)生成キーとした例である。

【0127】図19および図20に複数のデバイスに共通のコンテンツを送付した場合、それらのコンテンツの改竄の有無を検証するためのインテグリティ・チェック値生成キーKicvを有効化キープブロック(EKB)によって配信する構成例を示す。図19はデバイス0, 1, 2, 3に対して復号可能なチェック値生成キーKicvを配信する例、図20はデバイス0, 1, 2, 3中のデバイス3をリボーク(排除)してデバイス0, 1, 2に対してのみ復号可能なチェック値生成キーKicvを配信する例を示す。

【0128】図19の例では、更新ノードキーK(t)00によって、チェック値生成キーKicvを暗号化したデータ(b)とともに、デバイス0, 1, 2, 3においてそれぞれの有するノードキー、リーフキーを用いて更新されたノードキーK(t)00を復号可能な有効化キープブロック(EKB)を生成して配信する。それぞれのデバイスは、図19の右側に示すようにまず、EKBを処理(復号)することにより、更新されたノードキーK(t)00を取得し、次に、取得したノードキーK(t)00を用いて暗号化されたチェック値生成キー: Enc(K(t)00, Kicv)を復号してチェック値生成キーKicvを得ることが可能となる。

【0129】その他のデバイス4, 5, 6, 7...は同一の有効化キープブロック(EKB)を受信しても自身の保有するノードキー、リーフキーでは、EKBを処理して更新されたノードキーK(t)00を取得することができないので、安全に正当なデバイスに対してのみチェック値生成キーを送付することができる。

【0130】一方、図20の例は、図3の点線枠で囲んだグループにおいてデバイス3が、例えば鍵の漏洩によりリボーク(排除)されているとして、他のグループのメンバ、すなわち、デバイス0, 1, 2, に対してのみ復号可能な有効化キープブロック(EKB)を生成して配信した例である。図20に示す(a)有効化キープブロッ

ク(EKB)と、(b)チェック値生成キー(Kicv)をノードキー(K(t)00)で暗号化したデータを配信する。

【0131】図20の右側には、復号手順を示してある。デバイス0, 1, 2は、まず、受信した有効化キープブロックから自身の保有するリーフキーまたはノードキーを用いた復号処理により、更新ノードキー(K(t)00)を取得する。次に、K(t)00による復号によりチェック値生成キーKicvを取得する。

【0132】図3に示す他のグループのデバイス4, 5, 6...は、この同様のデータ(EKB)を受信したとしても、自身の保有するリーフキー、ノードキーを用いて更新ノードキー(K(t)00)を取得することができない。同様にリボークされたデバイス3においても、自身の保有するリーフキー、ノードキーでは、更新ノードキー(K(t)00)を取得することができず、正当な権利を有するデバイスのみがチェック値生成キーを復号して利用することが可能となる。

【0133】このように、EKBを利用したチェック値生成キーの配送を用いれば、データ量を少なくして、かつ安全に正当権利者のみが復号可能としたチェック値生成キーを配信することが可能となる。

【0134】このようなコンテンツのインテグリティ・チェック値(ICV)を用いることにより、EKBと暗号化コンテンツの不正コピーを排除することができる。例えば図21に示すように、コンテンツC1とコンテンツC2とをそれぞれのコンテンツキーを取得可能な有効化キープブロック(EKB)とともに格納したメディア1があり、これをそのままメディア2にコピーした場合を想定する。EKBと暗号化コンテンツのコピーは可能であり、これをEKBを復号可能なデバイスでは利用できないことになる。

【0135】図21の(b)に示すように各メディアに正当に格納されたコンテンツに対応付けてインテグリティ・チェック値(ICV(C1, C2))を格納する構成とする。なお、(ICV(C1, C2))は、コンテンツC1とコンテンツC2にハッシュ関数を用いて計算されるコンテンツのインテグリティ・チェック値である $ICV = hash(Kicv, C1, C2)$ を示している。図21の(b)の構成において、メディア1には正当にコンテンツ1とコンテンツ2が格納され、コンテンツC1とコンテンツC2に基づいて生成されたインテグリティ・チェック値(ICV(C1, C2))が格納される。また、メディア2には正当にコンテンツ1が格納され、コンテンツC1に基づいて生成されたインテグリティ・チェック値(ICV(C1))が格納される。この構成において、メディア1に格納された{EKB, コンテンツ2}をメディア2にコピーしたとすると、メディア2で、コンテンツチェック値を新たに生成するとICV(C1, C2)が生成されることになり、メディア

に格納されているKicv (C1) と異なり、コンテンツの改竄あるいは不正なコピーによる新たなコンテンツの格納が実行されたことが明らかになる。メディアを再生するデバイスにおいて、再生ステップの前ステップにICVチェックを実行して、生成ICVと格納ICVの一致を判別し、一致しない場合は、再生を実行しない構成とすることにより、不正コピーのコンテンツの再生を防止することが可能となる。

【0136】また、さらに、安全性を高めるため、コンテンツのインテグリティ・チェック値 (ICV) を書き換えカウンタを含めたデータに基づいて生成する構成としてもよい。すなわち $ICV = hash(Kicv, counter + 1, C1, C2, \dots)$ によって計算する構成とする。ここで、カウンタ (counter + 1) は、ICVの書き換えごとに1つインクリメントされる値として設定する。なお、カウンタ値はセキュアなメモリに格納する構成とすることが必要である。

【0137】さらに、コンテンツのインテグリティ・チェック値 (ICV) をコンテンツと同一メディアに格納することができない構成においては、コンテンツのインテグリティ・チェック値 (ICV) をコンテンツとは別のメディア上に格納する構成としてもよい。

【0138】例えば、読み込み専用メディアや通常のMO等のコピー防止策のとられていないメディアにコンテンツを格納する場合、同一メディアにインテグリティ・チェック値 (ICV) を格納するとICVの書き換えが不正なユーザによりなされる可能性があり、ICVの安全性が保てないおそれがある。この様な場合、ホストマシン上の安全なメディアにICVを格納して、コンテンツのコピーコントロール (例えばcheck-in/check-out、move) にICVを使用する構成とすることにより、ICVの安全管理およびコンテンツの改竄チェックが可能となる。

【0139】この構成例を図22に示す。図22では読み込み専用メディアや通常のMO等のコピー防止策のとられていないメディア2201にコンテンツが格納され、これらのコンテンツに関するインテグリティ・チェック値 (ICV) を、ユーザが自由にアクセスすることの許可されないホストマシン上の安全なメディア2202に格納し、ユーザによる不正なインテグリティ・チェック値 (ICV) の書き換えを防止した例である。このような構成として、例えばメディア2201を装着したデバイスがメディア2201の再生を実行する際にホストマシンであるPC、サーバにおいてICVのチェックを実行して再生の可否を判定する構成とすれば、不正なコピーコンテンツあるいは改竄コンテンツの再生を防止できる。

【0140】【階層ツリー構造のカテゴリー分類】暗号鍵をルートキー、ノードキー、リーフキー等、図3の階層ツリー構造として構成し、コンテンツキー、認証キ

ー、ICV生成キー、あるいはプログラムコード、データ等を有効化キーブロック (EKB) とともに暗号化して配信する構成について説明してきたが、ノードキー等を定義している階層ツリー構造を各デバイスのカテゴリー毎に分類して効率的なキー更新処理、暗号化キー配信、データ配信を実行する構成について、以下説明する。

【0141】図23に階層ツリー構造のカテゴリーの分類の一例を示す。図23において、階層ツリー構造の最上段には、ルートキーRoot 2301が設定され、以下の中間段にはノードキー2302が設定され、最下段には、リーフキー2303が設定される。各デバイスは個々のリーフキーと、リーフキーからルートキーに至る一連のノードキー、ルートキーを保有する。

【0142】ここで、一例として最上段から第M段目のあるノードをカテゴリノード2304として設定する。すなわち第M段目のノードの各々を特定カテゴリのデバイス設定ノードとする。第M段の1つのノードを頂点として以下、M+1段以下のノード、リーフは、そのカテゴリに含まれるデバイスに関するノードおよびリーフとする。

【0143】例えば図23の第M段目の1つのノード2305にはカテゴリ [メモリスティック (商標)] が設定され、このノード以下に連なるノード、リーフはメモリスティックを使用した様々なデバイスを含むカテゴリ専用のノードまたはリーフとして設定される。すなわち、ノード2305以下を、メモリスティックのカテゴリに定義されるデバイスの関連ノード、およびリーフの集合として定義する。

【0144】さらに、M段から数段分下位の段をサブカテゴリノード2306として設定することができる。例えば図に示すようにカテゴリ [メモリスティック] ノード2305の2段下のノードに、メモリスティックを使用したデバイスのカテゴリに含まれるサブカテゴリノードとして、[再生専用器] のノードを設定する。さらに、サブカテゴリノードである再生専用器のノード2306以下に、再生専用器のカテゴリに含まれる音楽再生機能付き電話のノード2307が設定され、さらにその下位に、音楽再生機能付き電話のカテゴリに含まれる

【PHS】ノード2308と【携帯電話】ノード2309を設定することができる。

【0145】さらに、カテゴリ、サブカテゴリは、デバイスの種類のみならず、例えばあるメーカー、コンテンツプロバイダ、決済機関等が独自に管理するノード、すなわち処理単位、管轄単位、あるいは提供サービス単位等、任意の単位 (これらを総称して以下、エンティティと呼ぶ) で設定することが可能である。例えば1つのカテゴリノードをゲーム機器メーカーの販売するゲーム機器XYZ専用の頂点ノードとして設定すれば、メーカーの販売するゲーム機器XYZにその頂点ノード以下の下

段のノードキー、リーフキーを格納して販売することが可能となり、その後、暗号化コンテンツの配信、あるいは各種キーの配信、更新処理を、その頂点ノードキー以下のノードキー、リーフキーによって構成される有効化キーブロック（EKB）を生成して配信し、頂点ノード以下のデバイスに対してのみ利用可能なデータが配信可能となる。

【0146】このように、1つのノードを頂点として、以下のノードをその頂点ノードに定義されたカテゴリ、あるいはサブカテゴリの関連ノードとして設定する構成とすることにより、カテゴリ段、あるいはサブカテゴリ段の1つの頂点ノードを管理するメーカー、コンテンツプロバイダ等がそのノードを頂点とする有効化キーブロック（EKB）を独自に生成して、頂点ノード以下に属するデバイスに配信する構成が可能となり、頂点ノードに属さない他のカテゴリのノードに属するデバイスには全く影響を及ぼさずにキー更新を実行することができる。

【0147】以上、特定の実施例を参照しながら、本発明について詳解してきた。しかしながら、本発明の要旨を逸脱しない範囲で当業者が該実施例の修正や代用を成し得ることは自明である。すなわち、例示という形態で本発明を開示してきたのであり、限定的に解釈されるべきではない。本発明の要旨を判断するためには、冒頭に記載した特許請求の範囲の欄を参酌すべきである。

【0148】

【発明の効果】以上、説明したように、本発明の情報処理システムおよび方法によれば、ツリー（木）構造の鍵配布構成により、コンテンツキーや認証キー、コンテンツチェック値生成キー、プログラムデータ等を有効化キーブロック（EKB）とともに送信する構成としたので、正当なデバイスにおいてのみ復号可能な暗号データ配信が可能となるとともに配信メッセージ量を小さく抑えることができる。

【0149】また、ツリー構造の暗号化キー、データ配信方式を用いてコンテンツキーや認証キー、コンテンツチェック値生成キー、プログラムデータ等を有効化キーブロック（EKB）とともに送信する構成において、さらに、共通鍵方式、あるいは公開鍵方式の認証処理を併用する構成とすれば、さらに安全なデータ配信が可能となる。

【0150】また、本発明の情報処理システムおよび方法によれば、コンテンツに対するインテグリティ・チェック値（ICV）をコンテンツを格納した記録媒体、あるいはその他のメディアに格納してコンテンツ改竄のチェック、あるいはコピーチェックを可能としたので、不正なコンテンツの流通を防止することが可能となる。

【0151】また、本発明の情報処理システムおよび方法によれば、ツリー構造の暗号化キー、データ配信方式において、階層ツリーをカテゴリ毎に分類して、各カテ

ゴリの管理する頂点ノード以下のノード、リーフを特定のデバイスに限定する構成としたので、各カテゴリの管理者が独自に有効化キーブロック（EKB）を生成して管理下にあるデバイスに対して配信することが可能となる。

【図面の簡単な説明】

【図1】本発明の情報処理システムの構成例を説明する図である。

【図2】本発明の情報処理システムにおいて適用可能な記録再生装置の構成例を示すブロック図である。

【図3】本発明の情報処理システムにおける各種キー、データの暗号化処理について説明するツリー構成図である。

【図4】本発明の情報処理システムにおける各種キー、データの配布に使用される有効化キーブロック（EKB）の例を示す図である。

【図5】本発明の情報処理システムにおけるコンテンツキーの有効化キーブロック（EKB）を使用した配布例と復号処理例を示す図である。

【図6】本発明の情報処理システムにおける有効化キーブロック（EKB）のフォーマット例を示す図である。

【図7】本発明の情報処理システムにおける有効化キーブロック（EKB）のタグの構成を説明する図である。

【図8】本発明の情報処理システムにおける有効化キーブロック（EKB）と、コンテンツキー、コンテンツを併せて配信するデータ構成例を示す図である。

【図9】本発明の情報処理システムにおける有効化キーブロック（EKB）と、コンテンツキー、コンテンツを併せて配信した場合のデバイスでの処理例を示す図である。

【図10】本発明の情報処理システムにおける有効化キーブロック（EKB）とコンテンツを記録媒体に格納した場合の対応について説明する図である。

【図11】本発明の情報処理システムにおける有効化キーブロック（EKB）と、コンテンツキーを送付する処理を従来の送付処理と比較した図である。

【図12】本発明の情報処理システムにおいて適用可能な共通鍵暗号方式による認証処理シーケンスを示す図である。

【図13】本発明の情報処理システムにおける有効化キーブロック（EKB）と、認証キーを併せて配信するデータ構成と、デバイスでの処理例を示す図（その1）である。

【図14】本発明の情報処理システムにおける有効化キーブロック（EKB）と、認証キーを併せて配信するデータ構成と、デバイスでの処理例を示す図（その2）である。

【図15】本発明の情報処理システムにおいて適用可能な公開鍵暗号方式による認証処理シーケンスを示す図である。

【図16】本発明の情報処理システムにおいて公開鍵暗号方式による認証処理を用いて有効化キープロック（EKB）と、コンテンツキーを併せて配信する処理を示す図である。

【図17】本発明の情報処理システムにおいて有効化キープロック（EKB）と、暗号化プログラムデータを併せて配信する処理を示す図である。

【図18】本発明の情報処理システムにおいて適用可能なコンテンツ・インテグリティ・チェック値（ICV）の生成に使用するMAC値生成例を示す図である。

【図19】本発明の情報処理システムにおける有効化キープロック（EKB）と、ICV生成キーを併せて配信するデータ構成と、デバイスでの処理例を示す図（その1）である。

【図20】本発明の情報処理システムにおける有効化キープロック（EKB）と、ICV生成キーを併せて配信するデータ構成と、デバイスでの処理例を示す図（その2）である。

【図21】本発明の情報処理システムにおいて適用可能なコンテンツ・インテグリティ・チェック値（ICV）をメディアに格納した場合のコピー防止機能を説明する図である。

【図22】本発明の情報処理システムにおいて適用可能なコンテンツ・インテグリティ・チェック値（ICV）をコンテンツ格納媒体と別に管理する構成を説明する図である。

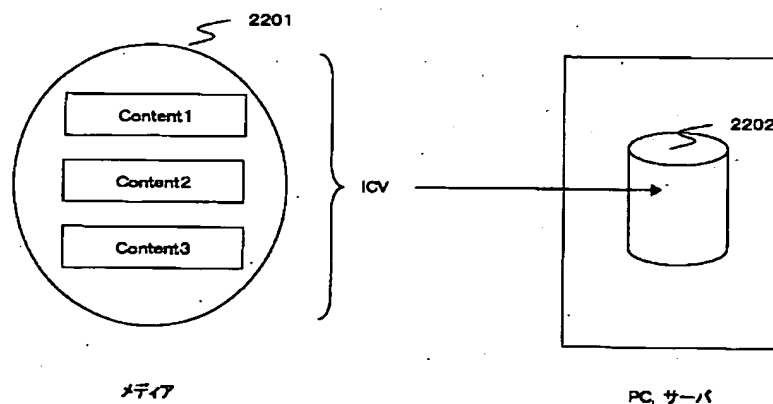
【図23】本発明の情報処理システムにおける階層ツリー構造のカテゴリ分類の例を説明する図である。

【符号の説明】

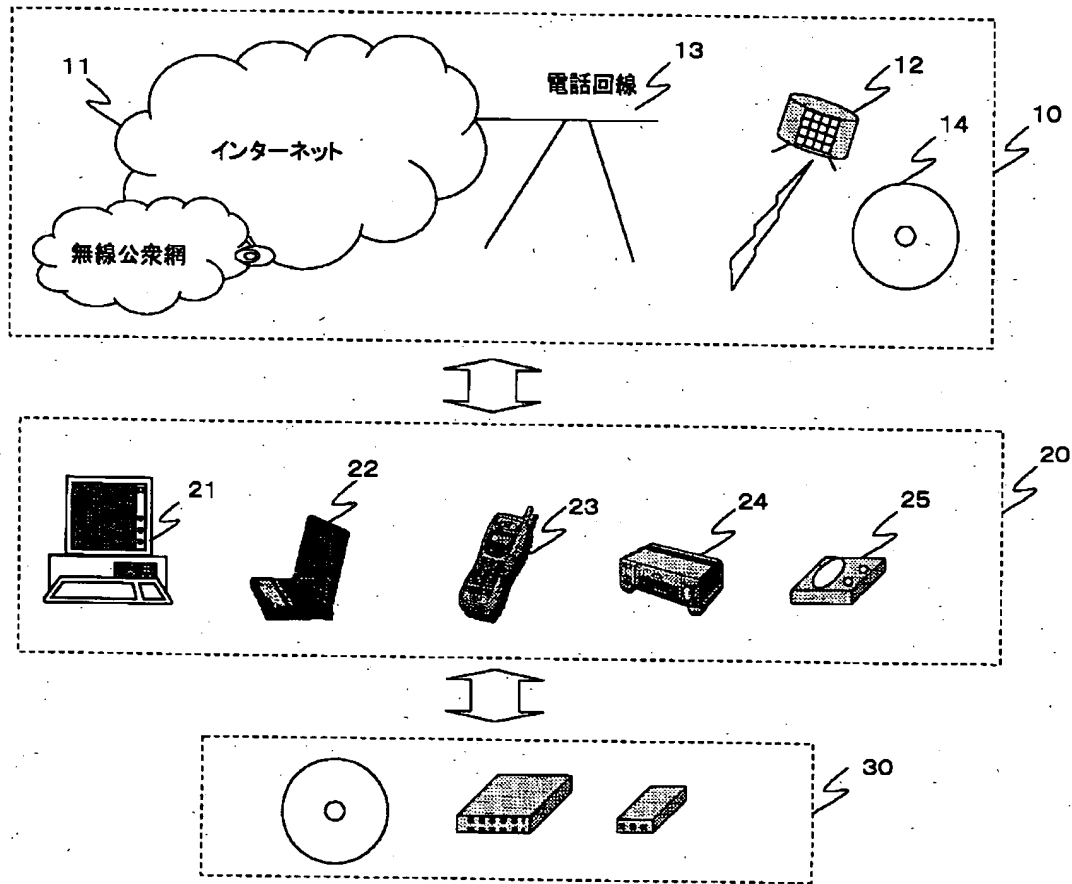
- 10 コンテンツ配信側
- 11 インターネット
- 12 衛星放送
- 13 電話回線
- 14 メディア

- 20 コンテンツ受信側
- 21 パーソナルコンピュータ（PC）
- 22 ポータブルデバイス（PD）
- 23 携帯電話、PDA
- 24 記録再生器
- 25 再生専用器
- 30 メディア
- 100 記録再生装置
- 110 バス
- 120 入出力I/F
- 130 MPEGコーデック
- 140 入出力I/F
- 141 A/D、D/Aコンバータ
- 150 暗号処理手段
- 160 ROM
- 170 CPU
- 180 メモリ
- 190 ドライブ
- 195 記録媒体
- 601 バージョン
- 602 デプス
- 603 データポインタ
- 604 タグポインタ
- 605 署名ポインタ
- 606 データ部
- 607 タグ部
- 608 署名
- 1101 記録デバイス
- 2301 ルートキー
- 2302 ノードキー
- 2303 リーフキー
- 2304 カテゴリノード
- 2306 サブカテゴリノード

【図22】



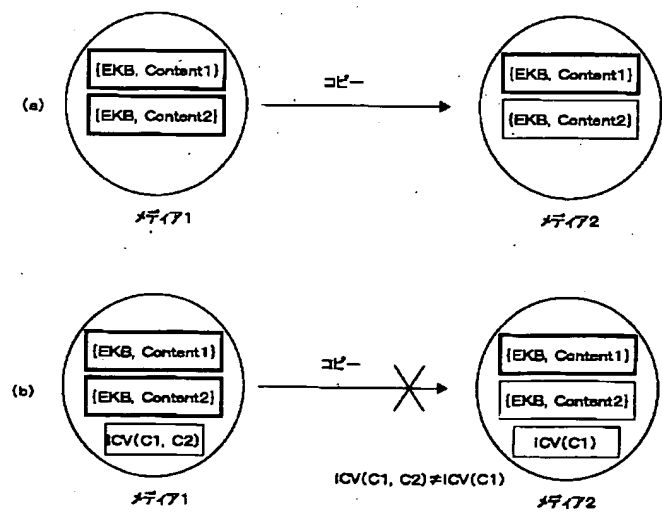
【図1】



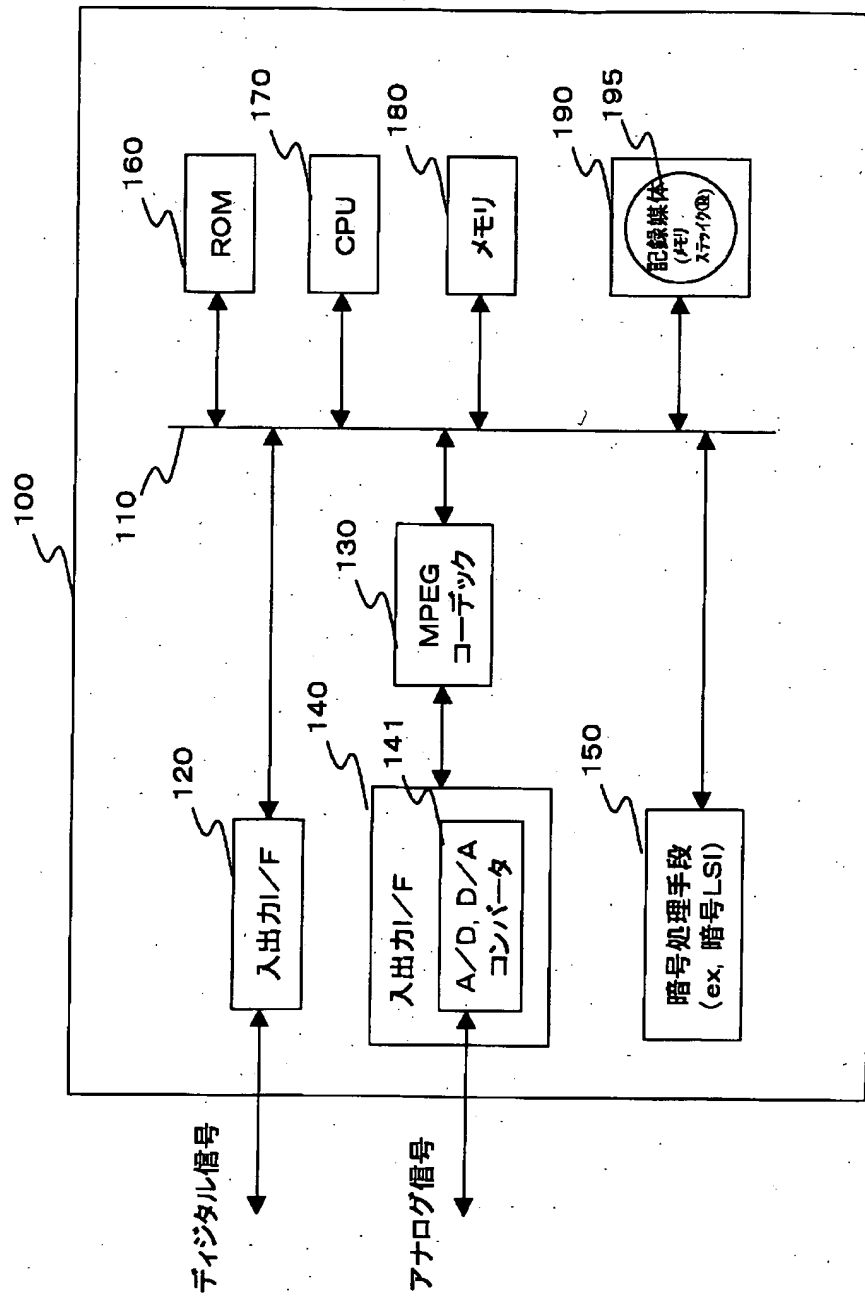
【図10】



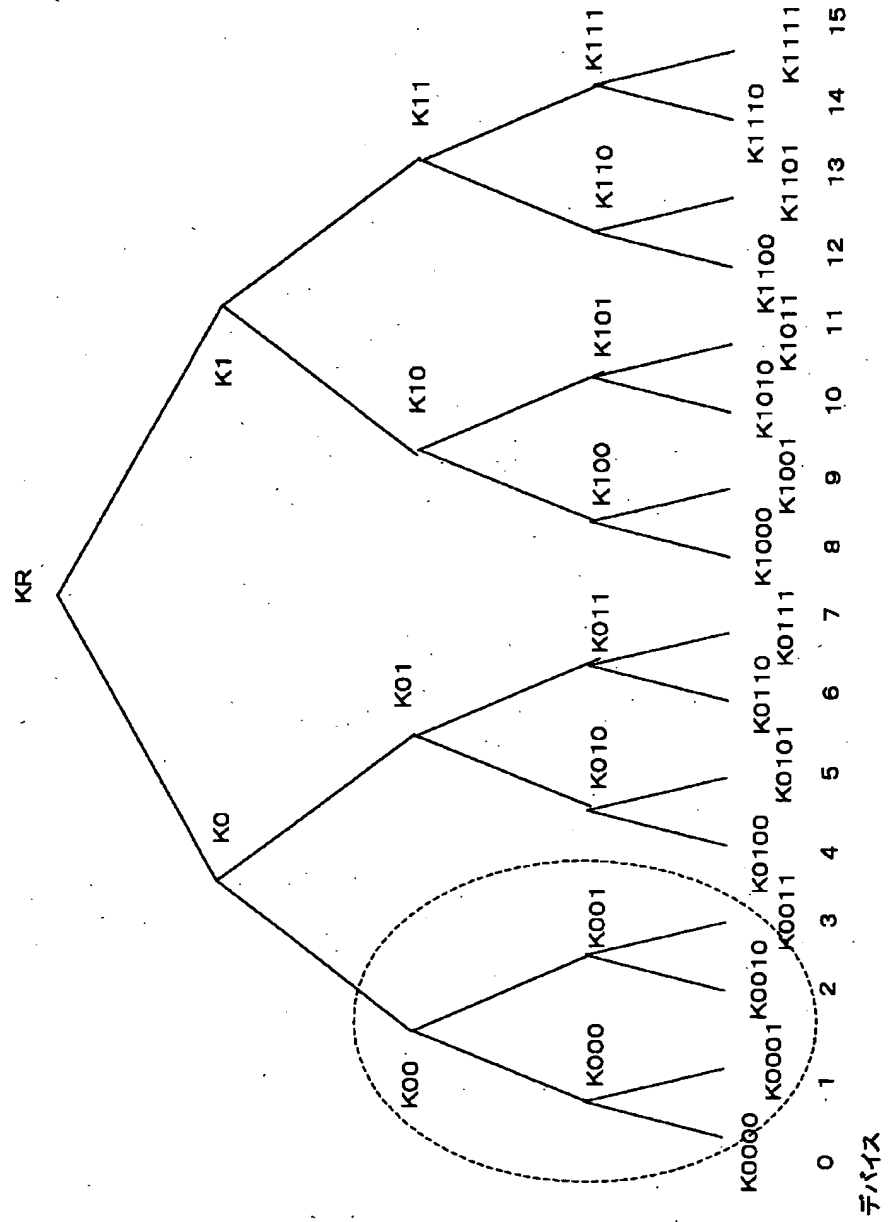
【図21】



【図2】



【図3】



【図4】

(A) 有効化キーブロック(EKB: Enabling Key Block) 例1

デバイス0, 1, 2にバージョン:tのノードキーを送付

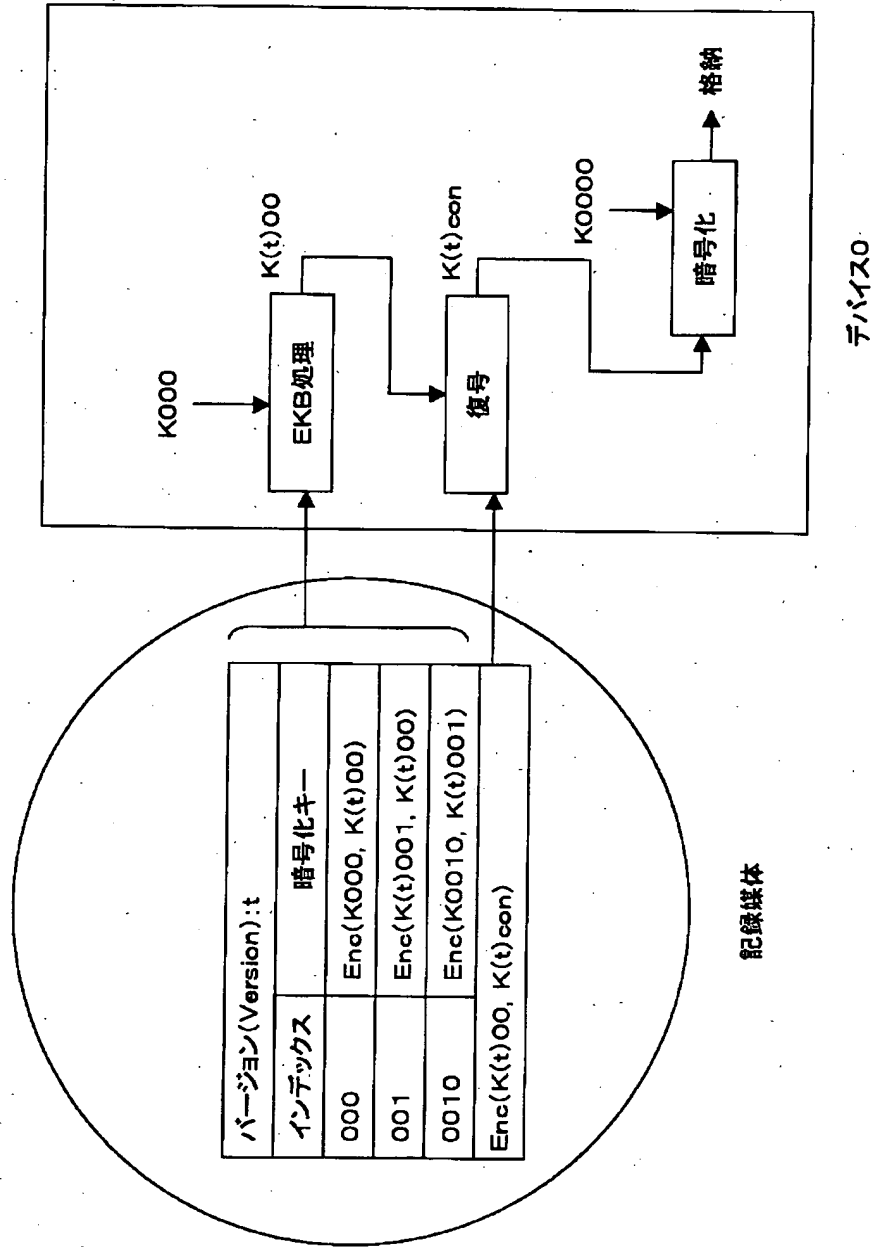
バージョン(Version):t	
インデックス	暗号化キー
0	Enc(K(t)0, K(t)R)
00	Enc(K(t)00, K(t)0)
000	Enc(K000, K(t)00)
001	Enc(K(t)001, K(t)00)
0010	Enc(K0010, K(t)001)

(B) 有効化キーブロック(EKB: Enabling Key Block) 例2

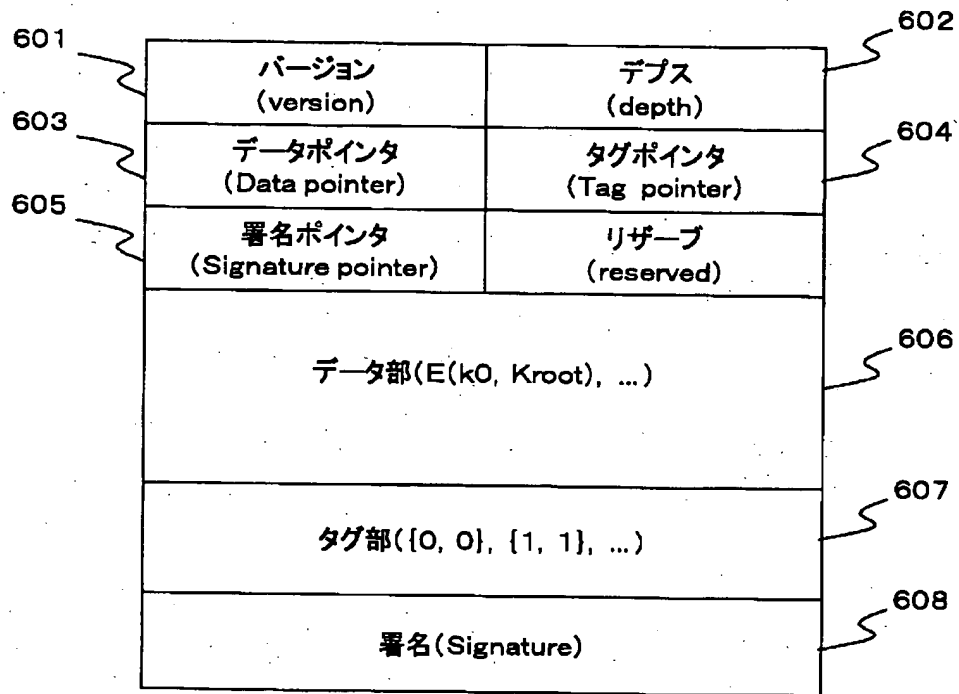
デバイス0, 1, 2にバージョン:tのノードキーを送付

バージョン(Version):t	
インデックス	暗号化キー
000	Enc(K000, K(t)00)
001	Enc(K(t)001, K(t)00)
0010	Enc(K0010, K(t)001)

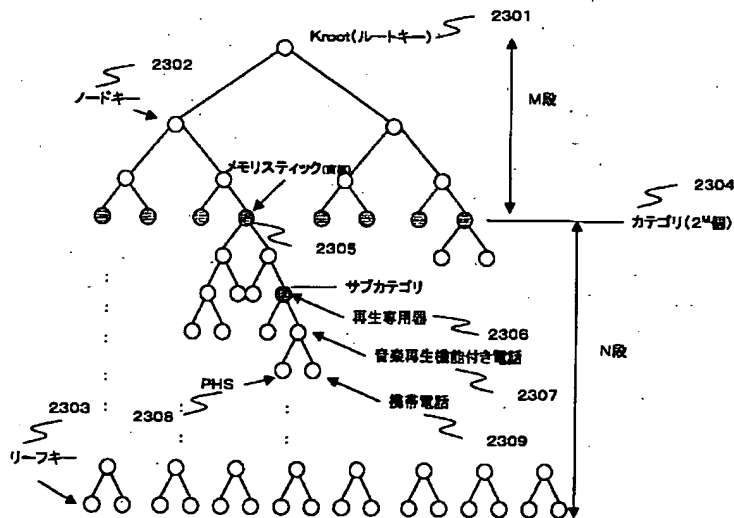
【図5】



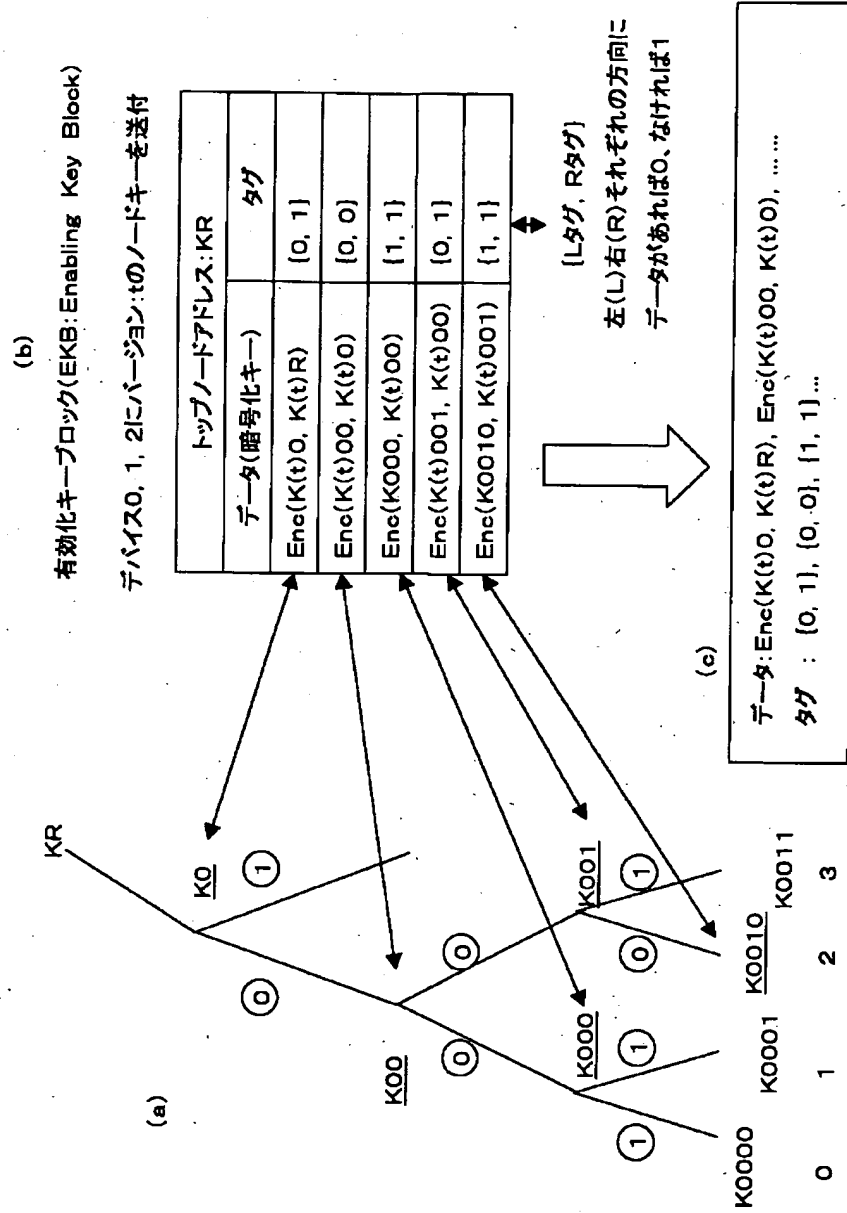
【図6】

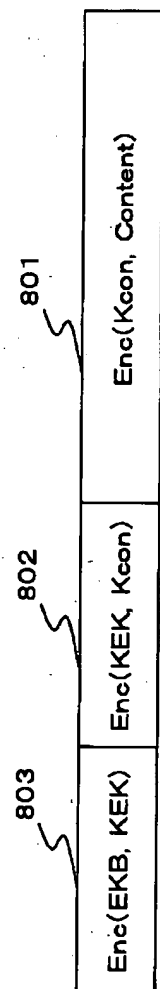


【図23】

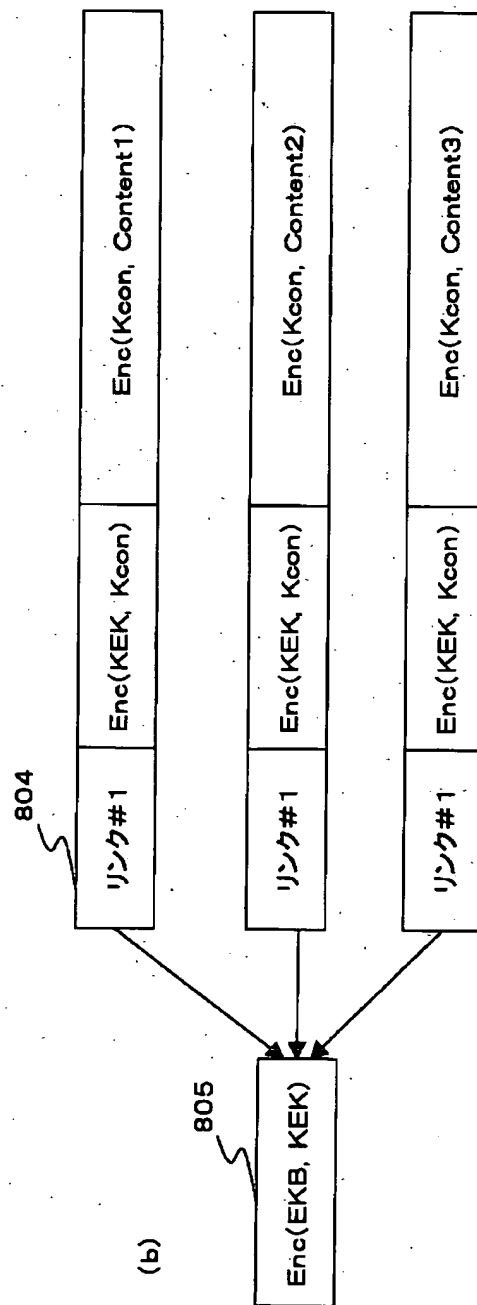


【図 7】



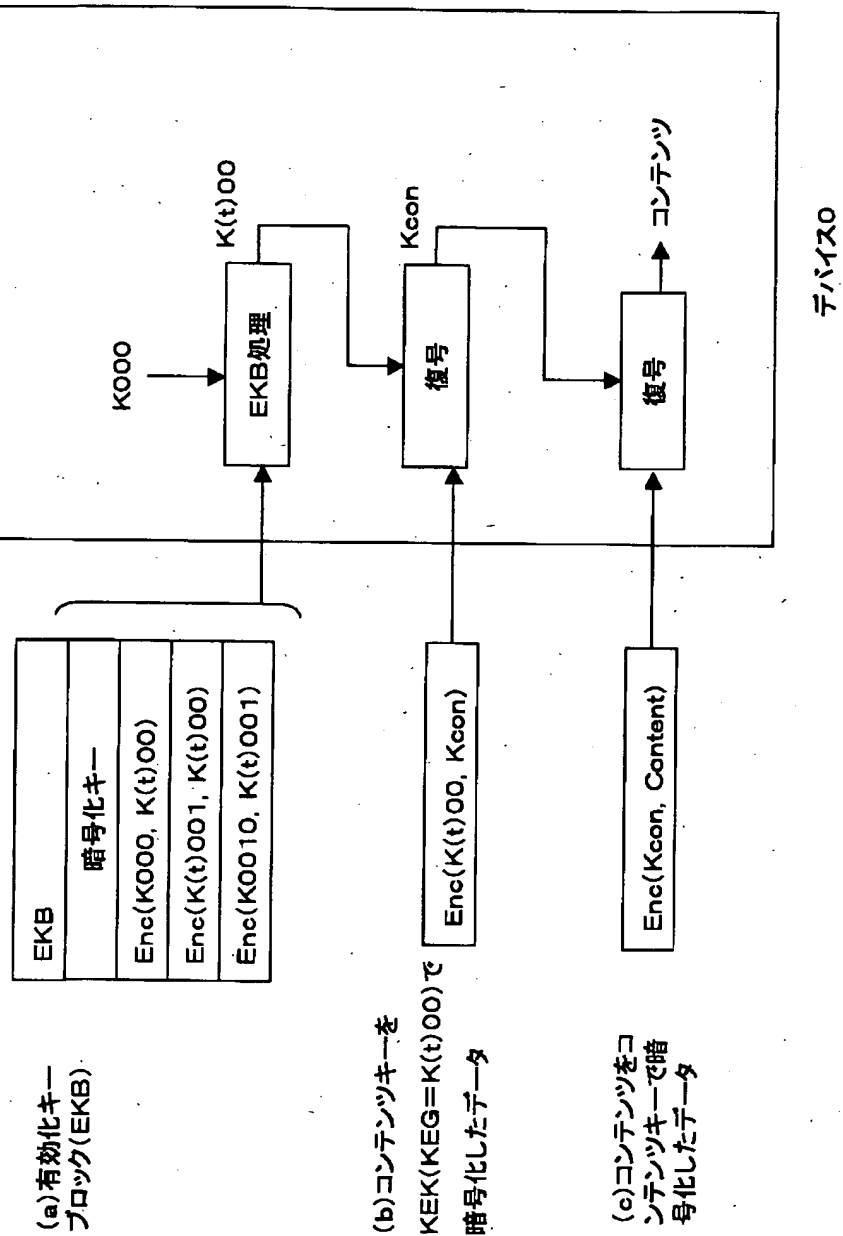


(a)



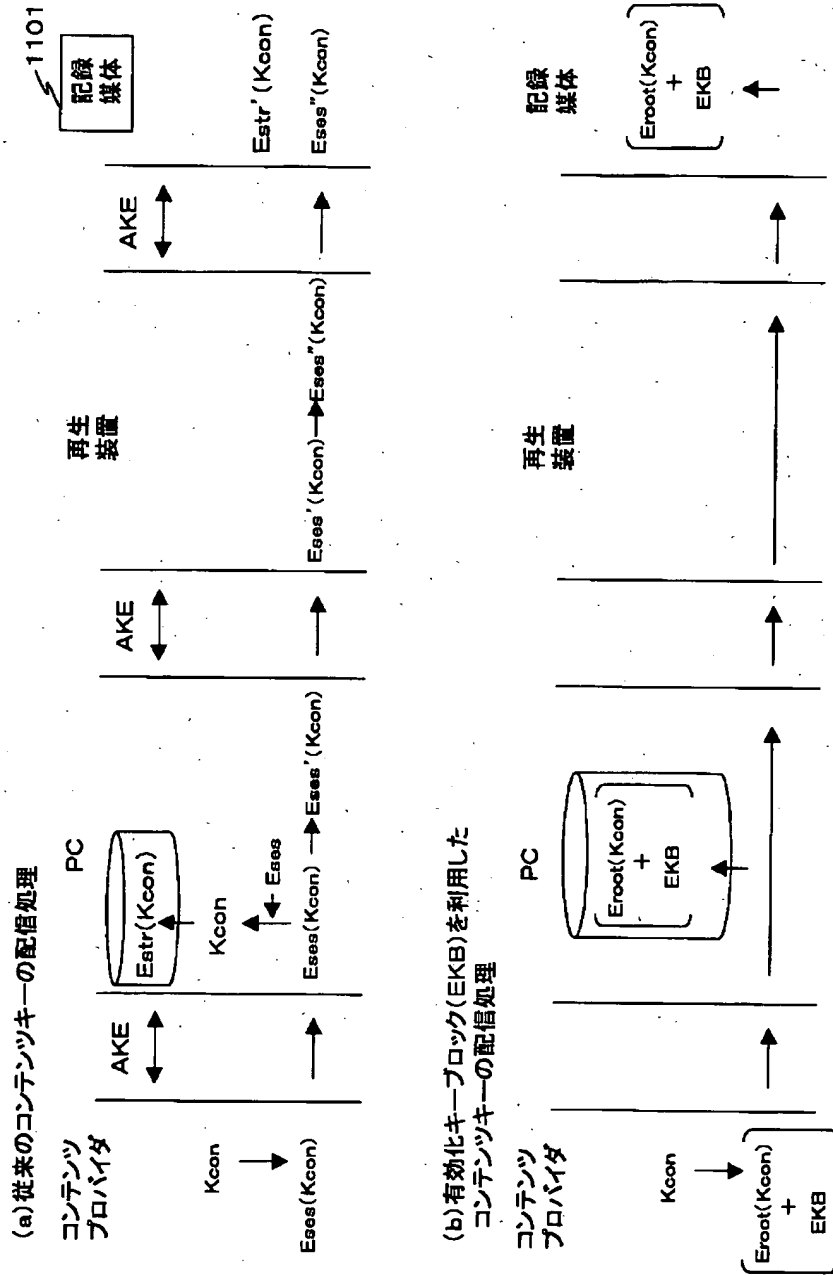
(b)

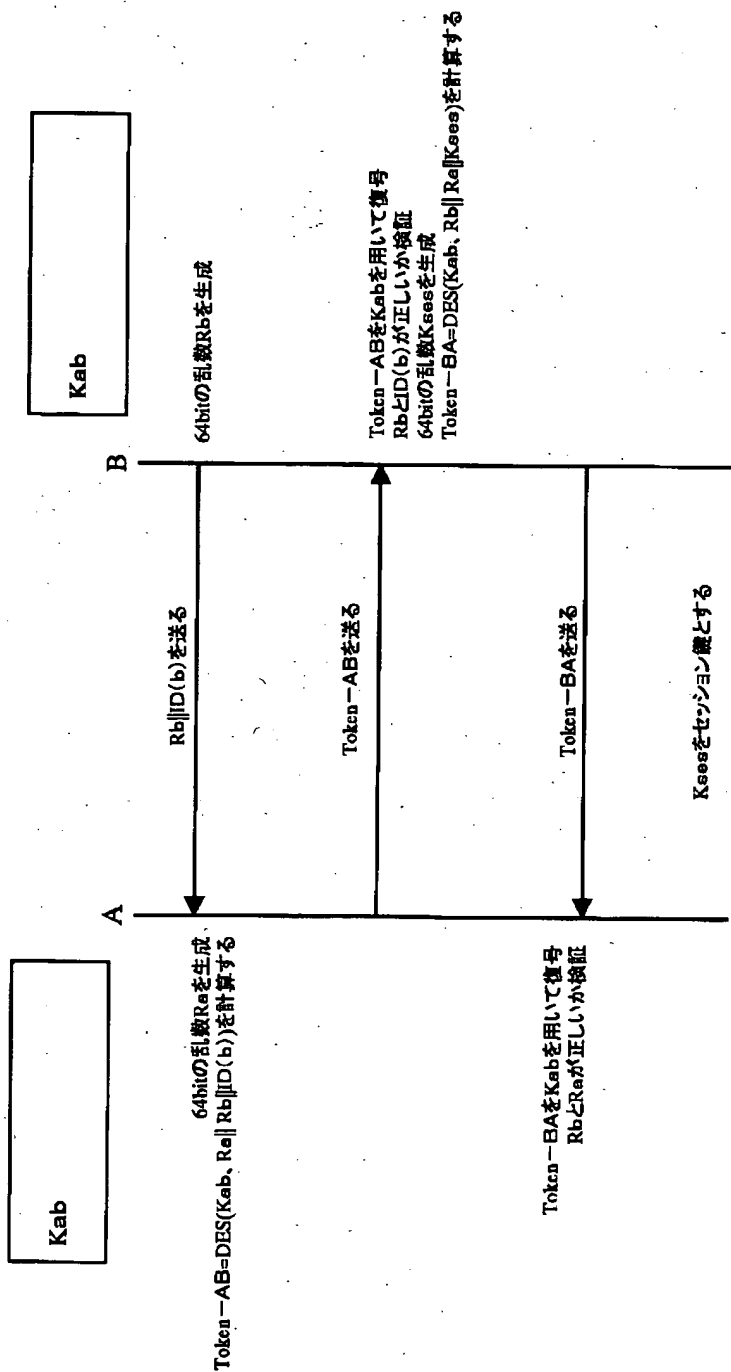
【図8】



【図9】

【図 11】

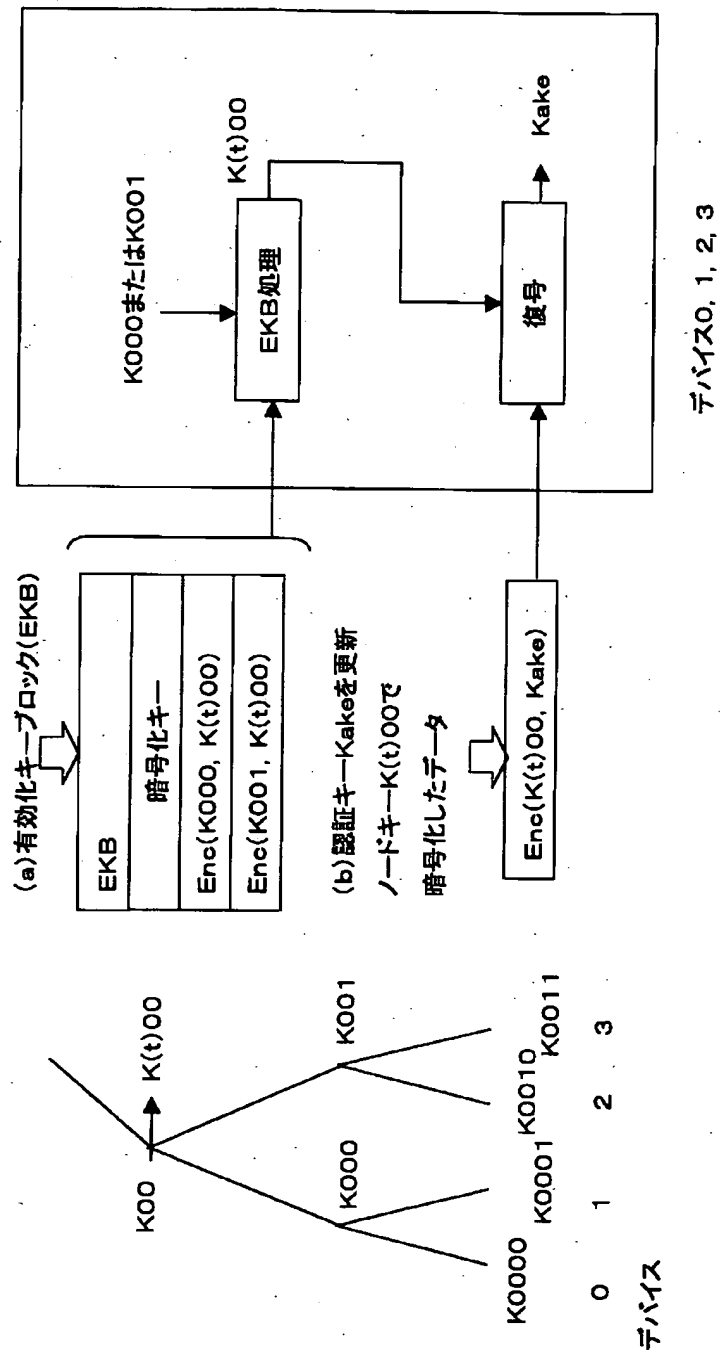




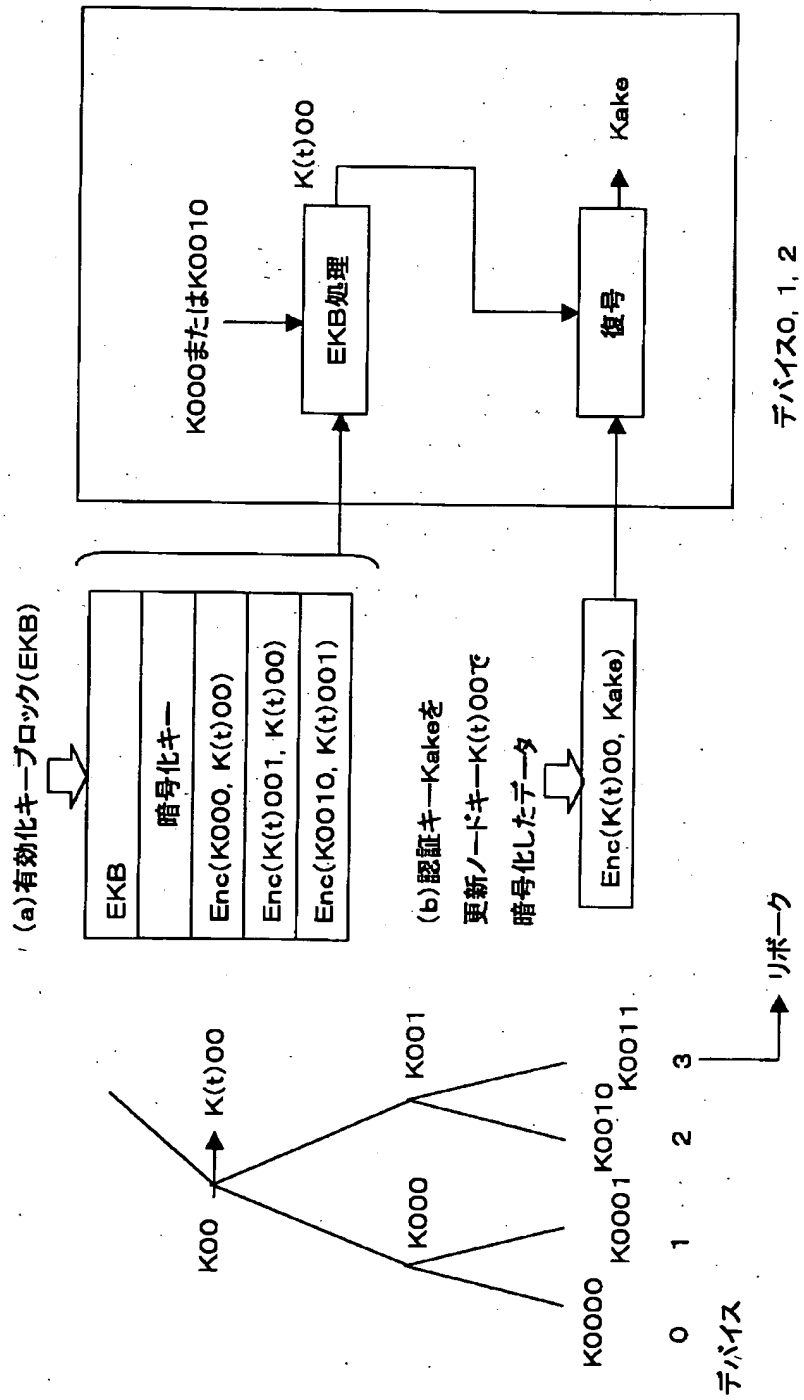
【図 12】

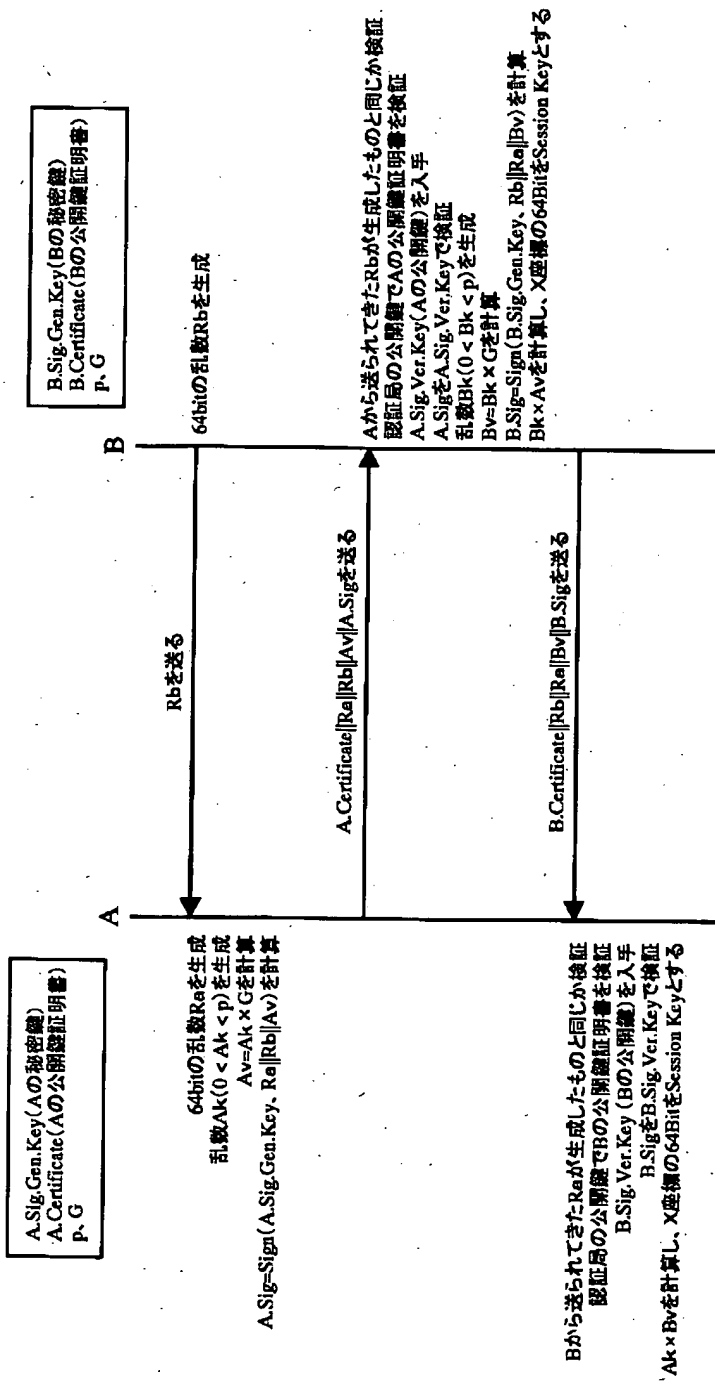
ISO/IEC 9798-2 対称鍵暗号技術を用いた相互認証および鍵共有方式

【図13】



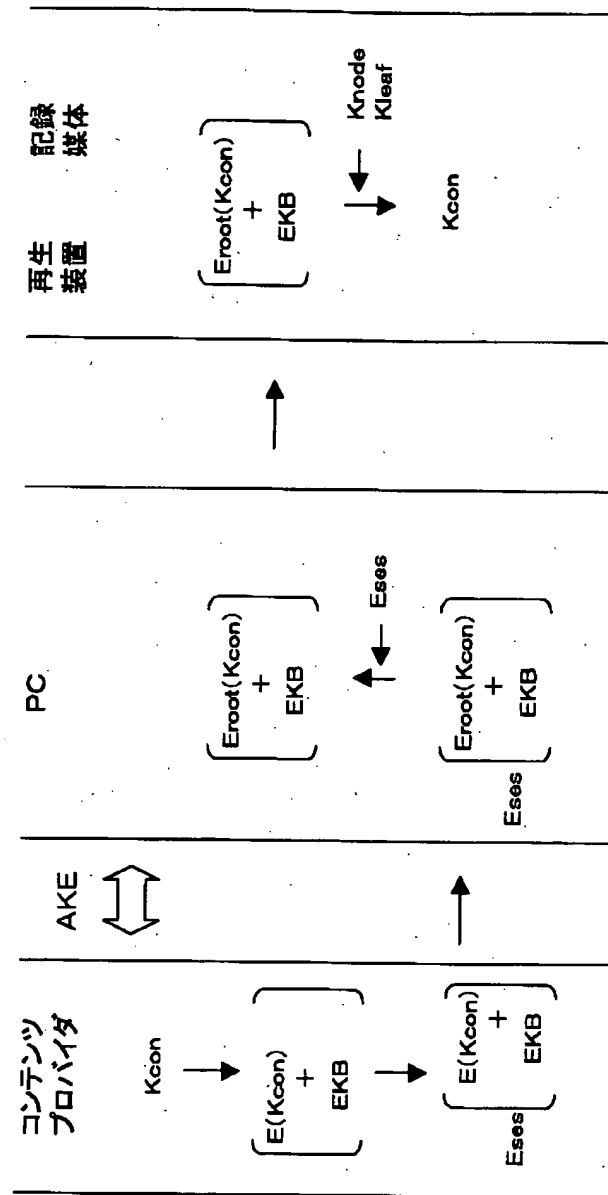
【図14】



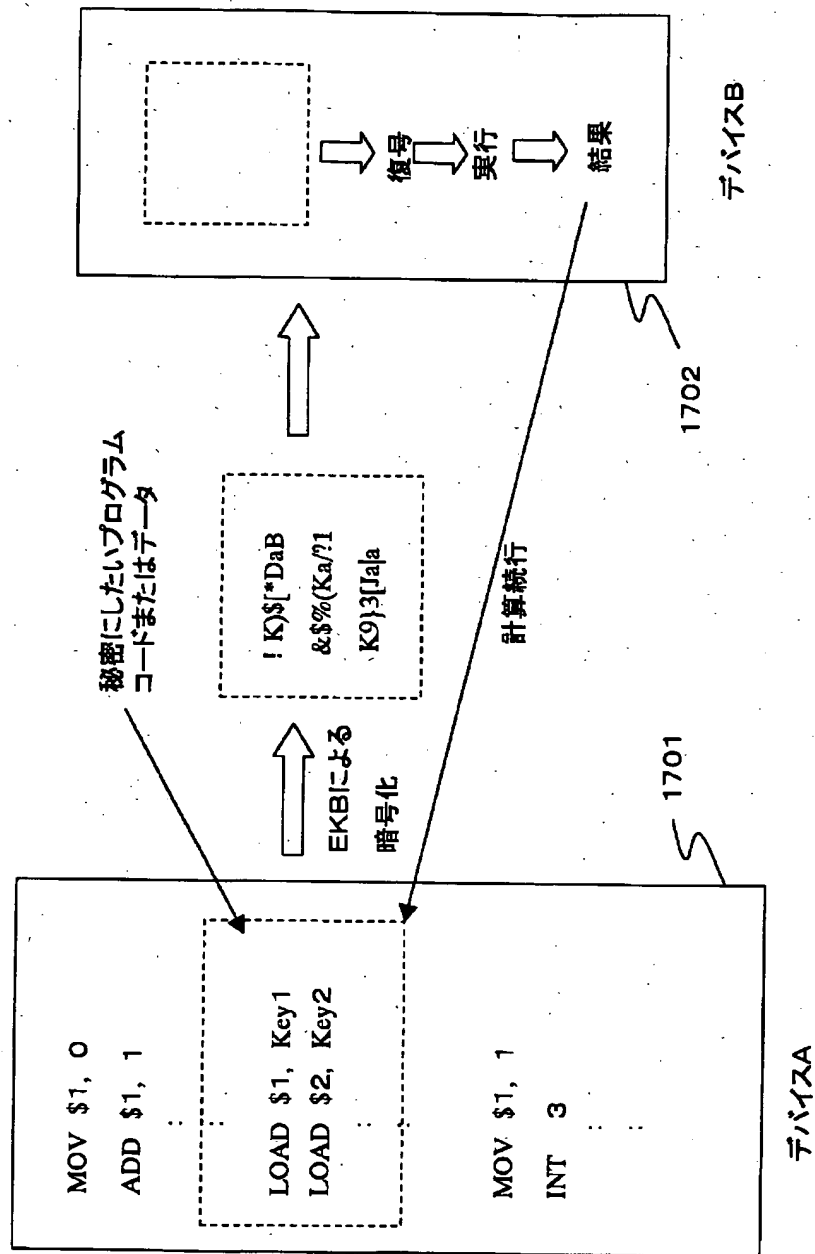


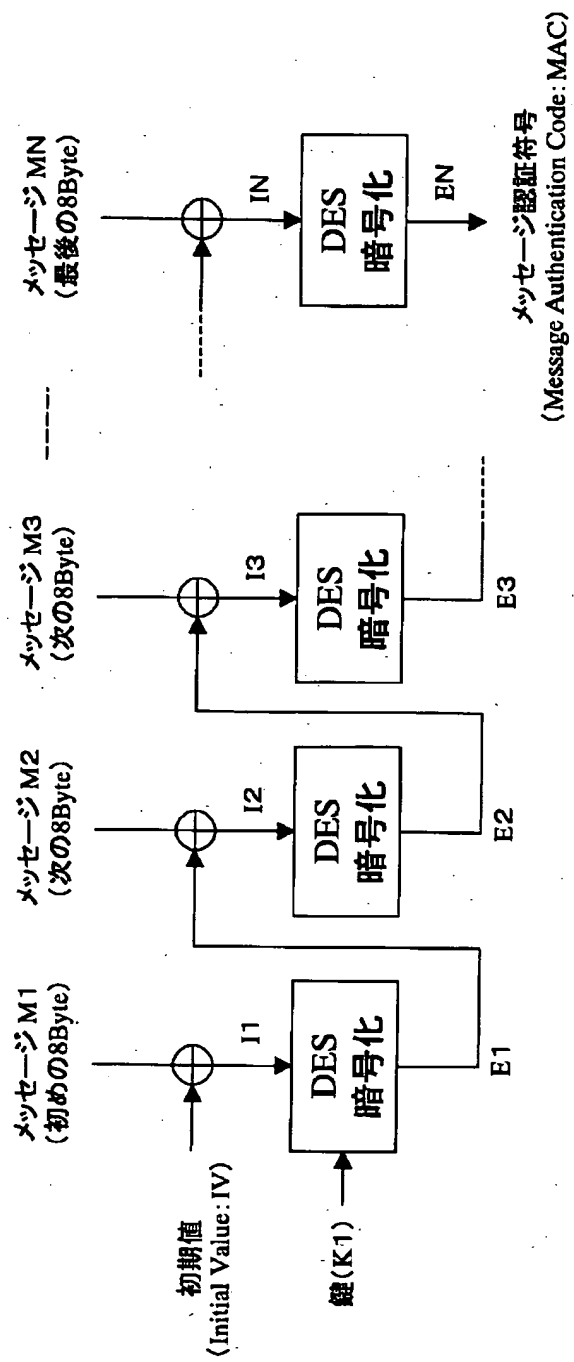
ISO/IEC 9798-3 非対称鍵暗号技術を用いた相互認証および鍵共有方式

【図16】



【図17】

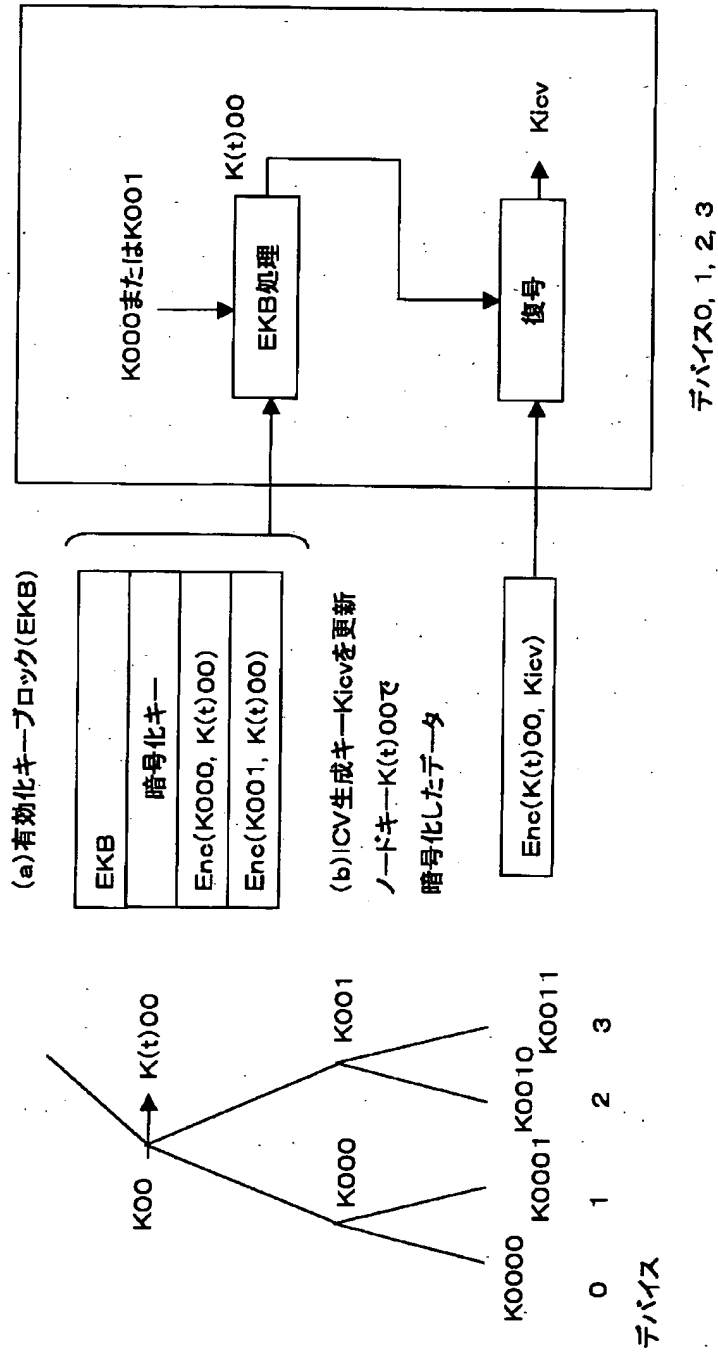




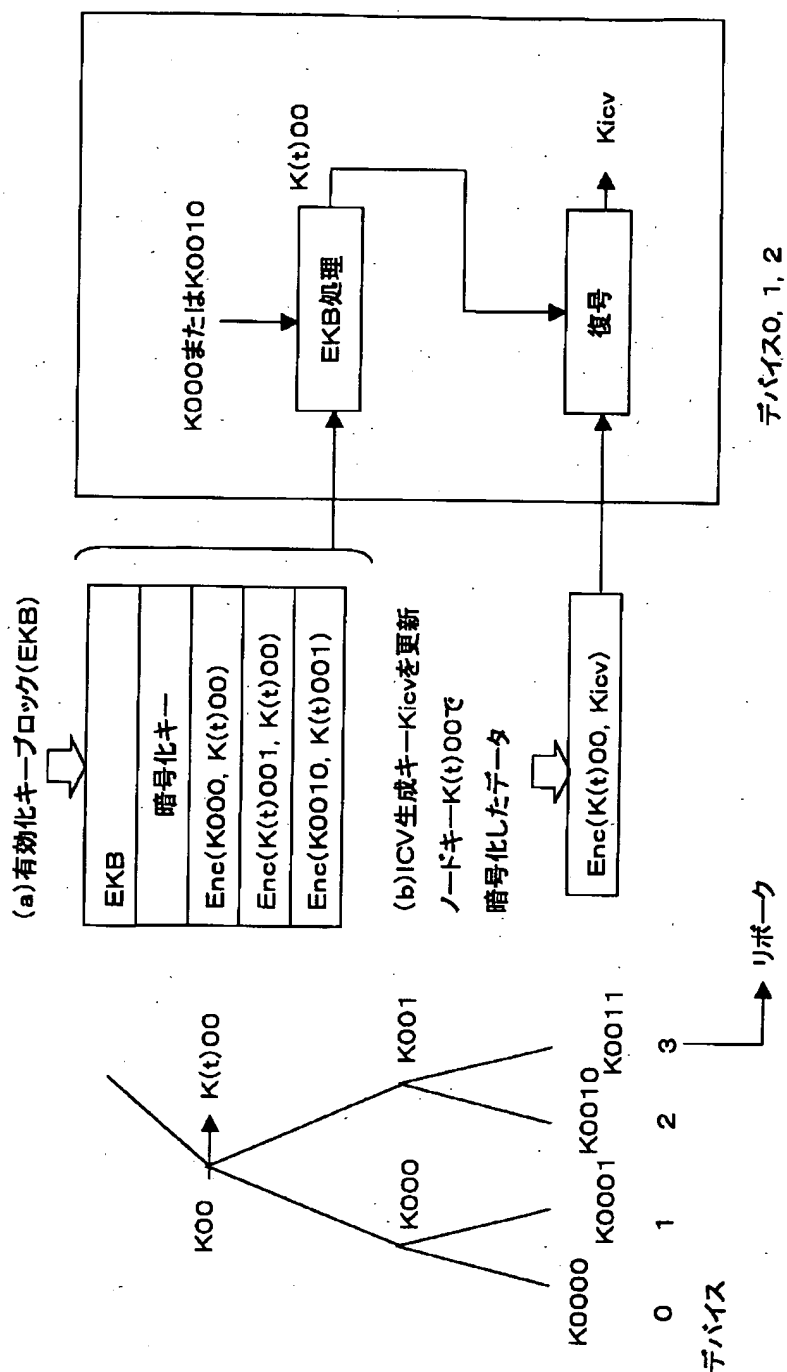
⊕ : 排他的論理和処理(8バイト単位)

【図18】

【図19】



【図20】



フロントページの続き

(72)発明者 大石 丈於
東京都品川区北品川6丁目7番35号 ソニ
ー株式会社内

(72)発明者 浅野 智之
東京都品川区北品川6丁目7番35号 ソニ
ー株式会社内

(72) 発明者 光澤 敦
東京都品川区北品川 6 丁目 7 番 35 号 ソニ
ー株式会社内

F ターム (参考) 5B017 AA07 BA07 CA09
5J104 AA01 AA12 AA16 EA02 EA07
EA17 NA03 NA27 PA07 PA10
PA14